КОМПЬЮТЕРРА
КОМПЬЮТЕРНЫЙ ЕЖЕНЕДЕЛЬНИК
13.11.07
#42 (710)

ПОД УДАРОМ

ЭКОНОМИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

14 ЭКУНЕТ НЕ ПОБЕДИЛА
работы вывозили на улицы

30 ХАКЕРЫ ПРОТИВ ПОКЕРА
реальности в играх и не только

30 3000 КРАТ 3 МЕГАПИКСЕЛА
почти «мыло» по рабочей этике

SHOUT
SHARE
IT

- Бумажная Компьютерра №42 (710)
- 13-я комната: Конструктор миров
- НОВОСТИ: Новости
- Микрофишки
- Босс есть босс
- Естественные процессы
- тема номера: Всепроникающая небезопасность
- Экономика без опасности
- книги: Недетские игры
- анализы: Машины для голосования в России
- наука: Наноалхимия
- голубятня: Мы встретились в аду
- опыты: Tor — круговая порука
- Охотники на инфузорий
- софтерра: Webология
- Софтерринки
- Патентное бюро
- TERRALAB.RU: Железный поток
- огород козловского: А я говорю: налево!
- письмоносец: Холодным субботним ноябрьским утром

Бумажная Компьютерра №42 (710)

Тема номера: Против лома

Выпускающий редактор: Владимир Гуриев
Дата выхода: 13 ноября 2007 года

13-я комната: Конструктор миров

Автор: Илья Щуров Voyager

Существенная часть сегодняшнего номера прямо или косвенно посвящена безопасности в самых разных ее проявлениях. Одним из факторов, про который часто вспоминают в этом контексте, является сравнительная анонимность современного Интернета. Фактор этот, впрочем, представляется то положительным, то отрицательным - в зависимости от позиции рассказчика. Мнения тут бывают прямо противоположные: одни люди обвиняют анонимность во всех смертных грехах и считают, что единственный способ остановить потоки вирусов, троянцев и спама, - поголовная "паспортизация Сети", другие, напротив, недовольны недостаточной анонимностью современного Интернета, позволяющей вести слежку за пользователями и "атаковать" их в реальной жизни (как, например, делает печально известная RIAA) - хотя последнее обычно и требует определенных усилий (получения санкции суда, обязующей провайдера раскрыть персональные данные).

Эти "другие" разрабатывают системы, позволяющие скрывать свою личность более эффективно. Филипп Казаков рассказывает про одну из самых популярных таких систем - Tor. Он сетует на нехватку места для более подробного рассказа, а также на недостаточную распространенность самого Tor'а. Я попробую отчасти исправить первую проблему - но усугубить вторую.

Для тех, кто читает журнал с начала, а не с конца, напомню, что Tor - система, позволяющая пользоваться Интернетом анонимно, подключаясь к серверам через цепочку промежуточных компьютеров. Одна из возможностей Tor'а, про которую Филипп ничего сказать не успел: так называемые скрытые сервисы, позволяющие соединять двух участников Сети таким образом, что ни один из них не знает IP-адреса другого. Тем самым анонимным остается не только, скажем, посетитель сайта, но и сам сайт (точнее - посетитель не знает, на каком сервере этот сайт располагается). Сама по себе техническая возможность подобной анонимной связи до сих пор вызывает у меня неподдельное восхищение - но, признаться, в ее практическое развитие я не верю. И вот почему.

Мы любим анонимность, когда речь идет о слежке за нами. Но мы тут же перестаем ее любить, когда не можем "вычислить" злобного спамера и написать жалобу его провайдеру или внести IP-адрес почтового сервера в черный список. Нам приятно думать о свободе слова, которую мы получаем с помощью технологий

вроде Tor’a - но вряд ли будет приятно узнать, что обнаружить хакера, взломавшего ваш банковский аккаунт, невозможно - причем невозможно принципиально, при всем желании правоохранительных органов вас защитить.

Уже сейчас tor-выходы блокируются разными сервисами "неанонимного" веба. И это, в общем-то, понятно: несмотря на все разговоры о свободе, очень хочется иметь хотя бы теоретическую возможность выйти на реального человека, если он что-то натворит. Придя в банк в маске, не стоит удивляться, что вас не принимают с улыбкой и не стремятся помочь: скорее всего полиция уже в пути. С распространением Tor’a эта ситуация только усугубится - и вскоре в "приличный веб" оттуда пускать просто перестанут (а если и не перестанут, то оставят доступ "только для чтения").

Остаются скрытые сервисы самого Tor’a. Но анонимный веб, развернутый в скрытых сервисах, вряд ли можно назвать подходящим местом для жизни. Например, в нем не может существовать Википедия - потому что бороться с вандализмом будет практически невозможно. И вряд ли анонимная почта будет пользоваться сильной популярностью - скорее всего разгул спамерской активности сведет всю пользу на нет. И уж точно никто не станет размещать интернет-магазин в подобной сети.

Коммуникативная составляющая, полагаю, будет убита. Останется лишь теоретическая возможность анонимной публикации материалов (что бывает действительно важным) - но как их можно будет распространить без почты, форумов, блогов?..

Тем не менее развитие подобных технологий - штука интереснейшая. Хотя бы потому, что она позволяет узнать больше о поведении людей в мирах с разным устройством - а значит, лучше понять самих себя.

НОВОСТИ: Новости

Звоните - открыто!

Оккупировав территорию онлайнового поиска и рекламы, а также заняв стратегические высоты среди веб-сервисов, компания Google устремила взгляд на многообещающий источник расширения аудитории - мобильники. Штурмовать новое направление в одиночку Google не отважилась и учредила мощную коалицию под названием Open Handset Alliance. Три десятка ее участников составляют операторы сотовой связи, производители чипов и мобильных телефонов. Знаменитых игроков в новоиспеченном альянсе немало, среди прочих в него входят Samsung, Intel, nVidia, LG, Motorola, HTC и eBay.

При всей своей решительности маневр Google был вполне ожидаемым; несколько месяцев пресса самозабвенно муссировала слухи о мобильных планах компании, порой даже подкрепляя свои догадки фотографиями "как бы прототипа" готовящегося телефона. Впрочем, конспиративным талантам Google со товарищи следует отдать должное, ведь несмотря на масштабность предприятия, о грядущем объединении уверенно заговорили лишь за пару дней до официального анонса.

Целью инициативы Google является разработка программной платформы (операционная система и приложения) для мобильных устройств, обеспечивающей небывалые возможности пользователям, простор для творческой мысли разработчикам приложений и провайдерам сотовой связи. Упор в будущей системе делается на доступ в Интернет, не уступающий по комфортности "большим" компьютерам. Компания взялась за программную реализацию платформы и пока не намерена выпускать мобильник под собственной маркой, доверив производство устройств партнерам, так что предвкушаемая многими "битва айфона и гуглофона" если не отменяется, то откладывается.

К экспансии в карманы сотовых абонентов гугловцы начали готовиться загодя, купив в 2005 году специализирующуюся на мобильном ПО компанию Android, основатель которой ныне руководит соответствующим направлением Google (проект получил по наследству имя "Android"). Во всех связанных с Open Handset Alliance сообщениях для прессы, да и в самом его названии, провозглашается открытость разрабатываемой платформы, которая будет базироваться на коде Linux, а

написанные в рамках проекта пользовательские приложения будут распространяться под Apache Software License (версия 2). На уже существующие модели телефонов Android, похоже, установить не удастся, во всяком случае без дополнительных ухищрений.

Преисполненный радужным настроением пресс-релиз не содержит никаких технических деталей, однако разработчики смогут оценить потенциал новинки уже в середине ноября, когда будет представлен предварительный вариант программного инструментария для Android. Выход же устройств на этой платформе запланирован на вторую половину следующего года.

Пока неизвестно, насколько сильно отразится появление Android на рынке платформ для умных телефонов, который сейчас поделен между Microsoft, Symbian, Palm, Apple и несколькими консорциумами, продвигающими портативные вариации Linux. Также неизвестно, чем, помимо открытости и, быть может, относительно низкой цены, Google собирается привлекать покупателей. Объявленное краеугольным камнем проекта полноценное использование ресурсов Интернета определяется не столько спецификой мобильных браузеров, сколько ограниченными аппаратными возможностями коммуникаторов и смартфонов, и как далеко в этом направлении продвинется альянс - большой вопрос.

Ставка на открытое программное обеспечение прочно связывает проект Google с конкурирующими платформами. Как стало известно, браузер, используемый в Android, построен на свободном движке WebKit, который является основой для штатного браузера Apple iPhone и Mac OS X, а также телефонов на Symbian Series 60. ИК

По обе стороны баррикад

Кража интеллектуальной собственности в Сети достигает угрожающих масштабов. Молодая компания Attributor предложила подписной сервис, который способен взять на себя роль защитника от любителей плодить контент методом copy-paste.

Поисковые роботы стартапа ежедневно индексируют около 100 млн. страниц. Пока сервис способен выявить только заимствование статей (путем сопоставления крупных блоков текста), проверка изображений и видео добавится в ближайшее время. При обнаружении фактов незаконного копирования в адрес сайта-нарушителя автоматически отправляется требование

об удалении материалов или добавлении ссылки на первоисточник.

Услугами Attributor уже пользуются крупнейшие информационные агентства - Reuters и Associated Press. Эти организации, ежедневные публикации которых исчисляются тысячами, несут ощутимые потери из-за того, что трафик уходит на сторону. Для обслуживания клиентов с более скромными запросами, например блоггеров, ревниво охраняющих свой контент, компания к следующему году подготовит облегченный пакет услуг стоимостью несколько долларов в месяц.

Борьба с пиратством идет по всем фронтам, однако по ту сторону баррикад тоже не дремлют. Крупнейший трекер The Pirate Bay готовит замену BitTorrent, давно ставшего кошмарным сном правообладателей (к поиску альтернативы принуждает планируемое BitTorrent Inc. добавление закрытых расширений протокола). Проект пока безымянный, с ходом работы можно ознакомиться на сайте www.securep2p.net. Информационные флибустьеры рассчитывают обеспечить надежный транспорт для передачи данных, уделив особое внимание обеспечению анонимности пользователей и защите от вредительства со стороны блюстителей копирайта. А3

Сервер и прочие домашние животные

Microsoft выпустила еще одну операционную систему. Речь идет о Windows Home Server (WHS), предназначенной для использования на домашних серверах и анонсированной Биллом Гейтсом на январской выставке CES.

На самом деле WHS незаметно появилась в продаже еще в октябре, а нынешнее объявление связано с началом приема предварительных заявок на продукт Hewlett-Packard - главного "железного" партнера Microsoft в этом проекте. Поскольку поставки HP MediaSmart Server должны начаться где-то к концу месяца, очевидно, что дата 4 ноября выбрана чисто формально, просто чтобы привлечь внимание потребителей.

WHS построена на основе Windows Server 2003 - функции последней, конечно, несколько урезаны в обмен на упрощение настройки и администрирования системы. Компьютеры с Home Server призваны играть роль координационного центра, ведающего домашними десктопами, ноутбуками и игровыми приставками Xbox. Сервер берет на себя задачи автоматического бэкапа дисков подшефного хозяйства, хранения файлов общего пользования (прежде всего медиатеки), а также обеспечения

удаленного доступа через веб-интерфейс к домашним ПК (покупателям системы предоставляется бесплатный доменный адрес в службе Windows Live). Для клиентских компьютеров под управлением Windows XP и Vista настройка соединения с WHS производится автоматически, пользователям прочих операционных систем придется поработать руками. Как и полагается настоящему серверу, WHS-компьютеру не требуется монитор и клавиатура, управление осуществляется с клиентских машин.

Windows Home Server можно купить как отдельно (и установить на какой-нибудь завалявшийся дома ПК), так и в составе готовых программно-аппаратных комплексов от Hewlett-Packard, Fujitsu Siemens, Gateway, Iomega, LaCie, Medion и других фирм. Многие из анонсированных этими компаниями продуктов вполне могут украсить домашний интерьер; правда, большинство WHS-систем появится в продаже только в конце текущего или начале следующего года.

Перспективы этого проекта Microsoft оценить пока трудно. С одной стороны, WHS довольно проста в использовании и нетребовательна к ресурсам компьютера (процессор как минимум гигагерцовый, 512 мегабайт оперативки и 70-гигабайтный винчестер). При нынешнем распространении ноутбуков, имеющих обыкновение теряться, удобная централизованная бэкап-система дома явно не повредит. Опять же теоретически ничто не мешает использовать WHS в качестве файлового и сервера печати в небольших компаниях (число клиентских подключений ограничено десятком). С другой стороны, Home Server пока вряд ли годится на роль массового продукта, он рассчитан скорее на продвинутых пользователей. А последние вполне могут предпочесть альтернативные решения (в том числе open source), пусть и более сложные в настройке. ВБ

Бедные тоже радуются

То, о чем так долго говорили в стенах Media Lab

Массачусетского технологического института, наконец, свершилось: "стодолларовые" ноутбуки пошли в массовое производство.

Выпуск портативных компьютеров XO организован на китайском заводе тайваньской компании Quanta Computer. По-видимому, одна из первых партий лэптопов отправится в Уругвай - правительство этой страны сделало заказ на 100 тысяч экземпляров. Кроме того, заинтересованность в недорогих машинах выразила Монголия. Заявки, сделанные гражданами США и Канады по программе "заплати за два ноутбука, получи один" (второй пойдет бедным детям), начнут удовлетворяться в декабре.

Следует отметить, что пока количество заказов на перспективный гаджет явно оставляет желать лучшего, да и его себестоимость по-прежнему чуть ниже двухсот долларов вместо запланированных ста. Вдобавок, по словам представителей проекта, цена может изменяться из-за дополнительных пользовательских опций, которые встраиваются в некоторых странах, а также колебаний цен на сырье.

Впрочем, сэкономить обладатели зеленого лэптопа смогут на другом - на электроэнергии. Не так давно OLPC объявил о ведущейся разработке дополнительного устройства к компьютеру. Ни "аксессуаром", ни "гаджетом" назвать его нельзя: не подходит это слово к зарядник у на пятнадцать батарей, создатели которого планируют использовать в качестве источника энергии для генератора "коровьи лепешки". Или можно присоединить к нему солнечную батарею: очень удобно, если розетки далеко, а солнца, наоборот, в избытке - как раз то, что нужно в Африке.

Проект, однако, прирастает не только зарядниками. Инициативу согласились поддержать Intel и Microsoft. Первая намерена выпустить новый мобильный процессор, предназначенный для использования в составе "стодолларовых" ноутбуков, а вторая - пытается адаптировать Windows XP для установки на маломощный компьютер (128 Мбайт оперативки и 512 Мбайт флэш-памяти вместо винчестера). Конечно, и Intel, и Microsoft преследуют прежде всего собственные интересы (сейчас в XO используются чипы AMD Geode и операционная система Linux), но возможно, и бедным странам от этого что-то перепадет.
ВГ ПП

ПК на свалку истории?

Анализ тенденций развития мирового рынка информационных технологий, проведенный авторитетной фирмой IDC, позволяет говорить о том, что в развитых странах интерес к персональным компьютерам медленно, но верно падает.

По данным IDC, в Японии уже пятый квартал подряд наблюдается сокращение объемов продаж ПК. Темпы роста поставок десктопов и ноутбуков замедляются и в Соединенных Штатах. Причиной тому, по мнению экспертов, появление все более функциональной бытовой техники и мощных портативных устройств. В современном цифровом доме набор из DVD-рекордера, плоскопанельного телевизора, игровой приставки и смартфона фактически может заменить развлекательный центр, роль которого раньше играл ПК. При этом пользоваться бытовыми устройствами зачастую удобнее, чем обычным компьютером, а смотреть на большой экран телевизора - приятнее.

О приближающемся конце эры персональных компьютеров визионеры говорят не первый год. Например, прошлой осенью глава компании Symbian Найджел Клиффорд (Nigel Clifford) заявил, что через пять лет традиционные настольные компьютеры будут уже мало кому нужны, а на смену ноутбукам придут коммуникаторы. Горячие новинки этого года - Apple iPhone и операционная система для портативных устройств Google Android, - кажется, только подтверждают подобные прогнозы.

Впрочем, далеко не факт, что с эпохой ПК пора прощаться. Япония в технологическом отношении, конечно, "впереди планеты всей", но островное общество столь своеобразно, что не может служить надежной моделью для прочих развитых стран. Опять же нельзя забывать о "третьем мире", где, напротив, наблюдается бурный рост объемов поставок компьютеров. А инициативы вроде проекта OLPC (см. заметку "этажом выше") должны и вовсе привести к глобальной компьютеризации бедных регионов. ВГ

Все что ни делается, делается в Китае

Компания Lenovo планирует отправить на свалку истории брэнд IBM. Конечно, для того, чтобы стереть эти три буквы со всех электронных устройств будущего, необходимы ресурсы, которых у китайского гиганта пока нет. Речь идет лишь о той доле бизнеса IBM, которая была продана фирме Lenovo в 2004 году. Однако именно эта часть наиболее близка обычному человеку, дома или на работе у которого отведено место для настольного компьютера или ноутбука.

В договоре между Lenovo и IBM о покупке производства персональных компьютеров есть пункт, оставляющий за китайцами право использовать брэнд IBM для этой продукции до 2010 года. От этого права компания и решила отказаться досрочно, а именно в 2008-м. Возможно, искать причины происходящего стоит не только в успехах Lenovo, которая вышла в третьем квартале текущего года на рекордный для себя уровень прибыли, но и в таком, на первый взгляд, не относящемся к делу обстоятельстве, как пекинская олимпиада-2008. Lenovo, конечно, вошла в число спонсоров соревнований и, видимо, решила использовать ситуацию с максимальной выгодой. В преддверии главного спортивного форума фирма планирует провести рекламную кампанию по ребрэндингу, которую так или иначе пришлось бы делать к 2010 году, но уже без столь яркого фона, как олимпиада.

Однако другое наследие от IBM в виде названия серии ноутбуков ThinkPad решено оставить. В китайской компании полагают, что это обеспечит преемственность и сохранит зарубежных клиентов. Таким образом, брэнд Lenovo ThinkPad, который и будет продвигаться, возможно, станет переходным и поможет закрепить в умах покупателей название фирмы. Ну а навязшее в зубах в восьмидесятые годы словосочетание "компьютеры IBM PC/XT с любой периферией" окончательно уйдет в прошлое. АБ

Типа англим

Бесчисленные упреки прессы, тринадцать тысяч обозленных клиентов и девять месяцев судебного разбирательства потребовалось для того, чтобы крупнейший мобильный оператор США Cellco Partnership (торговая марка Verizon Wireless) прилюдно признал, что фактически занимался подлогом. История началась с год назад, когда Verizon развернула агрессивную

рекламную кампанию высокоскоростного интернет-доступа без проводов и без ограничений. Согласно рекламе, за 60–80 долларов (дешевле, если беспроводная карта или телефон, поддерживающие 3G-стандарт EVDO, приобретались у самой Verizon) клиент получал в неограниченное пользование канал скоростью примерно полмегабита в секунду. Однако для множества клюнувших на рекламу радость быстро сменялась удивлением: сотни "новообращенных" уже через месяц были отключены, договоры с ними разорваны, и число "отщепенцев" продолжало расти.

Сопоставив все имевшиеся факты - в частности, подозрение, что "режут" самых активных клиентов, и письма от Verizon с предупреждением о "необычно высокой интернет-активности", полученные частью пользователей, - сообщество недовольных, наконец, обратило внимание на правила предоставления услуг. Тут-то и выяснилось, что тарифы, рекламировавшиеся как "анлимитед", на деле "анлимитед не совсем". В лучших традициях жанра, мелким шрифтом в глубине документов были спрятаны истинные условия - обрамленные массой невообразимых в век YouTube ограничений. Так, счастливым безлимитчикам запрещалось играть в игры, слушать веб-радио и смотреть потоковое видео, качать мультимедийные подкасты, пользоваться файлообменными системами и т. п. и т. д. В перечне разрешенных остались лишь электронная почта, веб-серфинг, да доступ к интранету по месту работы, и то суммарным объемом не больше 5 гигабайт в месяц. Когда же пораженные клиенты обращались в компанию с просьбой объяснить, почему такие условия называются тарифами без ограничений, пресс-служба Verizon нимало не смущаясь выдавала отлуп в стиле "если Вы заглянете в сопроводительные документы, то, конечно, поймете, что речь идет о неограниченных объемах данных для ограниченного количества типов данных".

К счастью для обманутых пользователей, дело происходило не в российской глубинке, а в Америке. Так что в какой-то момент терпение общественности лопнуло, и власти штата Нью-Йорк организовали расследование деятельности компании. Решением по которому стало признание рекламы Verizon "вводящей в заблуждение" и требование полностью компенсировать пострадавшим клиентам их затраты (на сумму более чем в миллион долларов), да еще и уплатить в бюджет штата штраф на 150 тысяч долларов. Впрочем, Verizon и тут сумела сделать хорошую мину, лишь слегка подредактировав тексты документов (убрав пресловутое "без ограничений") и подав это как добровольное решение компании, продиктованное

"неустанной заботой о благе клиентов".

Российская же глубинка упомянута не случайно. В то время как Москва и Санкт-Петербург купаются в роскоши дешевых и действительно неограниченных тарифных планов на доступ в Сеть, в провинции царит настоящий произвол провайдеров. Автор этой заметки, проживающий в Екатеринбурге, сам не раз был свидетелем того, как компании от мала до велика (включая крупнейшего регионального игрока) под видом безлимитки продавали мало что смыслящим в предмете обывателям тарифные планы с казуистическими ограничениями и штрафами за "превышения". Быть может, пора и нам устроить показательную порку? EЗ

И швец, и жнец, и на дуде игрец

Пока поклонники продукции Apple восхищаются возможностями iPhone, а аналитики обсуждают перспективы выпуска новой мобильной платформы Google Android, японский телекоммуникационный гигант NTT DoCoMo представил два десятка сотовых телефонов третьего поколения с нестандартной функциональностью.

Скажем, в некоторых моделях старшего семейства 905i разработчики реализовали систему автоматического перевода. Все, что требуется от владельца, это произнести нужную фразу в микрофон, и через несколько секунд на дисплее появится ее версия на другом языке. Сам мобильник переводами, конечно, не занимается - все операции выполняются сервером. Нельзя не упомянуть и специальную интерактивную систему Chokkan Game, благодаря которой осуществлять управление в играх можно при помощи голосовых команд или путем изменения положения

телефона в пространстве. Интересны также "телевизионные" модели: Panasonic Viera P905iTV и Sharp Aquos SH905iTV с 3,5-дюймовыми экранами 480x854 способны принимать и записывать передачи цифрового наземного телевидения.

В большинстве устройств новой серии реализована поддержка информационного сервиса Area mail, с помощью которого рассылаются уведомления о прогнозируемых землетрясениях и других катаклизмах. Причем такие сообщения получают не все пользователи, а лишь те, которые в данный момент находятся в зоне потенциального риска. В отличие от обычных SMS или e-mail эти предупреждения сразу отображаются на экране аппарата и сопровождаются специальным звуковым сигналом. ВГ

Сколько вешать в терабайтах?

Американский суд удовлетворил коллективный иск к Seagate, в котором крупнейший производитель жестких дисков обвинялся в преднамеренном обмане покупателей путем применения некорректной системы подсчета объема накопителей.

Не секрет, что производители винчестеров, да и других носителей информации, нередко маркируют выпускаемые устройства в соответствии с десятичной системой исчисления, полагая, что один килобайт содержит 1000 байт. Однако операционные системы интерпретируют килобайт как 1024 байта. Таким образом, из-за некорректной маркировки покупатель в среднем недополучает семь процентов обещанной емкости жесткого диска. В случае с накопителями небольшого объема разница не слишком заметна. Однако по мере увеличения емкости "потери" становятся все более значительными. Так, например, в случае с винчестером, для которого количество "десятичных" гигабайт составляет 1000 (1 Тбайт), покупатель на самом деле получит только около 930 Гбайт дискового пространства.

В апреле 2005 года Seagate был предъявлен иск, на разбирательство по которому ушло два с половиной года. Ответчики согласились вернуть американским потребителям пять процентов от суммы, которая была заплачена при покупке винчестера. На компенсацию могут рассчитывать пользователи, купившие жесткие диски Seagate в период с 22 марта 2001 года по 26 сентября 2006 года. В качестве альтернативы денежной компенсации предлагается бесплатная копия программного

пакета Seagate Software Suite, который продается за 40 долларов. Правда, решение суда распространяется лишь на накопители, проданные отдельно. Иными словами, покупатели, получившие винчестер Seagate в составе готового компьютера, потребовать деньги или программу Seagate Software Suite не смогут.

Кстати, ранее обвинения в завышении емкости накопителей на жестких дисках были выдвинуты против крупнейших производителей ПК - Apple, Dell, Gateway, HP, IBM, Sharp, Sony и Toshiba. Окончательное решение по данному делу пока не вынесено. ВГ

Семнадцатое мгновение осени

Возможно ли научить машину мыслить? Пока философы и психологи ломают копья, пытаясь хоть как-то подобраться к этой проблеме, рыцари софта, засучив рукава, ваяют программы, способные прикинуться разумным собеседником. Как водится, "говорунов" по осени считают: в конце октября в Нью-Йорке традиционно прошел "финал четырех", по итогам которого лучшая программа-собеседник была удостоена ежегодной премии Лёбнера (www.loebner.net/Prizef/loebner-prize.html).

Престижная награда вручалась ныне уже в семнадцатый раз. По неукоснительно соблюдаемой традиции для выяснения степени "человекоподобия" программных говорунов члены жюри поочередно общались с двумя собеседниками, один из которых живой человек, а другой - бездушный бот, пытаясь выяснить, "кто есть ху". Правда, в последние годы задача программистов осложнилась еще одним условием: "набирать" генерируемый текст боту требуется на глазах своего собеседника, создавая у него иллюзию посимвольного ввода с клавиатуры и допускаемых человеком "очепяток". Понятно, что при этом чтение обычных "стенограмм" разговоров не позволяет ощутить атмосферы состязания. Поэтому, идя навстречу онлайновым болельщикам, организаторы выложили на своем сайте программу на Perl, позволяющую, как с кинопленки, в реальном времени "прокрутить" содержимое судейских мониторов во время сеанса связи.

Из финальной четверки лучше всех запудрить комиссии мозги удалось боту Ultra Hal Assistant. Имя он получил в честь знаменитого бортового компьютера HAL 9000, описанного Артуром Кларком в "Одиссее 2001". Подобно своему знаменитому прообразу, робот снабжен распознавателем и синтезатором речи, благодаря чему общаться с ним можно не только набирая фразы

на клавиатуре. Помимо голосового, он обладает и визуальным воплощением, представая в виде нескольких трехмерных аватаров, среди которых кроме человеческих типажей имеются говорящий монитор и улыбчивая лягушка. К чести "говоруна года", он способен вести не только досужие, но и деловые беседы, отзываясь на запросы типа "какой телефон у Иван Иваныча?" и напоминая хозяину о запланированных на день событиях.

Для продвижения своего детища 24-летний Роберт Метекса (Robert Meteksza) создал специальную компанию Zabaware. Коробочная версия говорящего электронного секретаря обойдется в 30 долларов. Желающие побеседовать с роботом "за жизнь" могут сделать это бесплатно, зайдя на сайт компании. При этом говорун доступен сразу в нескольких ипостасях - на одном и том же самообучающемся движке "выращены" боты, поддерживающие разговоры на самые разные темы. Так, среди них есть "эксперт по хомячкам", готовый часами говорить с вами об этих грызунах; ученик, впитывающий фразы своего собеседника как губка; а также плод коллективного педагогического труда досужих интернетчиков - "хулиган", напичканный экспрессивной лексикой. Желающие могут поселить Хэла и на своем собственном сайте. Полнофункциональный "швейцар" обойдется в 400 "зеленых", а любителям халявы положен "потолок обучения": база данных бота ограничена половиной мегабайта, да и общаться с ним придется через крохотное окошко, нашпигованное рекламой.

"Серебро" завоевал бот Cletus Ноя Данкэна (Noah Duncan), которого, как и год тому назад, подвела излишняя лаконичность фраз и страсть к однозначным ответам на вопросы. Триумфаторша предыдущих двух лет, Joan Ролло Карпентера (Rollo Carpenter), на сей раз довольствовалась "бронзой".

Разоряться хозяину премии пока не пришлось: и на сей раз все члены жюри безошибочно "отделили мух от котлет", выведя на чистую воду своих виртуальных собеседников. Так что при размере гран-при в сто тысяч долларов победителю, как обычно, достались лишь поощрительные две тысячи. Впрочем, этим дивиденды нынешнего чемпиона отнюдь не исчерпываются: в течение нескольких суток после финала на домашний сайт "Хэла" было не пробиться из-за обилия желающих перекинуться с ним словечком. А славу, как известно, за деньги не купишь. ДК

Гарри Поттер и лунный камень

Слухи о смерти Гарри Поттера в очередной раз оказались преувеличенными. В данном случае речь идет не о самом герое, а о затянувшейся эпопее под авторством Джоан Роулинг.

Оказывается, Джоан сочинила еще семь романов - все они, по ее словам, существуют в единственном экземпляре и являются рукописными. Гарри Поттера на их страницах, скорее всего, встретить не удастся, речь там не о нем. Зато эти "дополнения", объединенные под общим названием "The Tales of Beedle the Bard", были прорекламированы, как бы между прочим, в заключительной части похождений Поттера. Книга с таким названием в мире колдунов и ведьм является настольной, и наверное, каждый почитатель творчества Роулинг захотел бы иметь такую у себя дома. Но не тут-то было.

Повторимся, что каждая из частей магического сборника сказок уникальна и не будет печататься огромным тиражом. Более того, книги вообще не будут печататься, а так и найдут своих хозяев, оставаясь рукописями, проиллюстрированными самим автором. Шесть книг писательница подарит близким людям, наиболее тесно связанным с циклом произведений о Поттере. А седьмую Роулинг собирается продать в благотворительных целях.

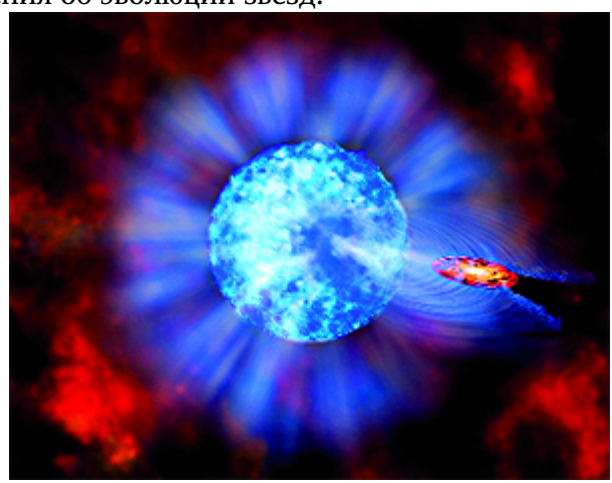
Покупателем опять-таки станет не счастливое издательство, которое смогло бы уже без всякой благотворительности "поделиться радостью" с остальным миром. Книга также не будет подлежать тиражированию и найдет самого фанатичного поклонника на аукционе Сотбис в середине декабря. Необычный рождественский подарок любой состоятельный человек сможет приобрести не меньше, чем за 30 тысяч фунтов (а скорее всего куда как дороже). Книга оформлена в соответствии с содержанием, облачена в сафьяновый переплет и украшена несколькими лунными камнями.

Не боясь ошибиться, можно предсказать, что на Роулинг обрушится град виртуальных камней, ведь это уже второй удар

ниже пояса, вслед за недавним заявлением писательницы о том, что Альбус Дамблдор был геем. Мало того что старые книги теперь придется переосмысливать, так и новые в руки не дают. АБ

Дыра не вписывается

Необычайно массивную черную дыру в двойной звездной системе недавно удалось обнаружить международной команде астрофизиков с помощью 8,2-метрового телескопа Gemini North, который расположен на самой высокой горе Гавайских островов Мауна-Кеа. Масса этой черной дыры почти в шестнадцать раз больше массы Солнца, что заставляет переосмыслить наши представления об эволюции звезд.



Астрономам повезло дважды. Мало того, что найденная ими черная дыра находится сравнительно недалеко, в небольшой расположенной по соседству с нами спиральной галактике Messier 33. Так эта дыра еще и быстро вращается вокруг очень массивной звезды, которая примерно в семьдесят раз тяжелее Солнца. Один оборот, аналогичный нашему году, черная дыра делает за три с половиной дня и при вращении может полностью заслоняться звездой или наоборот проходить перед ней. При таком вращении рентгеновское излучение аккреционного диска почти полностью перекрывается, и по его колебаниям можно достаточно точно оценить массу обоих объектов. Пока это первая черная дыра, найденная в такой двойной системе.

Цифра в шестнадцать солнечных масс плохо вписывается в современные модели звездной эволюции и образования черных дыр. Дело в том, что когда термоядерное горючее даже очень массивной звезды выгорает, она начинает сжиматься гравитацией

и затем взрывается, рождая сверхновую звезду. В этом сложном процессе только малая часть массы старой звезды остается в ее центре, формируя черную дыру, а основная доля вещества достается оболочке и уносится взрывом. Теория предсказывает, что так могут рождаться черные дыры с массой не больше десяти солнечных масс, а тут уже шестнадцать. Существует гипотеза, что в центрах галактик находятся очень массивные черные дыры с массой более тысячи солнечных, но механизм их образования пока остается загадкой (хотя, разумеется, в гипотезах нет недостатка).

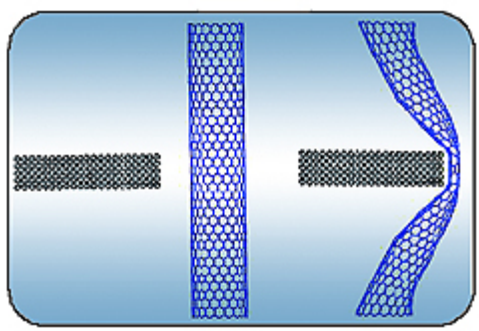
Впрочем, теоретики вскоре нашли правдоподобное объяснение большой массы обнаруженной черной дыры. Спектральный анализ излучения ее звезды показал, что она состоит из сравнительно чистого водорода и гелия. Примесей более тяжелых элементов в ней на порядок меньше, чем в нашем Солнце. А при таком составе звезды меняется характер взрыва сверхновой, что может, в принципе, привести к другому разделению масс между оболочкой и центром.

Теперь астрономы будут усердно искать аналогичные двойные объекты во вселенной, чтобы набрать хоть какую-то статистику по размерам черных дыр, а теоретикам придется подновить и пересчитать свои модели взрывов сверхновых. ГА

Бронеколготки

Углеродные нанотрубки могут стать прекрасной основой для нового поколения бронежилетов. К такому выводу пришли ученые из Сиднейского университета, делавшие расчеты баллистического удара по нанотрубкам методом молекулярной динамики.

Идея использовать прочные и легкие углеродные нанотрубки в бронежилетах давно витала в воздухе. Но идея - это одно, а готовый бронежилет - совсем другое. Из каких нанотрубок и как лучше его делать? От каких пуль он сможет защитить? Первые ответы на эти вопросы недавно сумели получить в Австралии.



Для простоты ученые сначала ограничились одной закрепленной на концах нанотрубкой и рассчитали, как она поведет себя при встрече с миниатюрной алмазной "пулей", на несколько порядков более тяжелой, чем трубка. Расчеты велись методом молекулярной динамики, в котором вычисляется движение каждого атома углерода. Оказалось, что одна нанотрубка способна противостоять "пуле", летящей со скоростью до двух километров в секунду, что вдвое быстрее, нежели при выстреле из винтовки в упор. При этом нанотрубка не разрушается, а сначала сминается и сгибается, а затем, распрямляясь как пружина, отбрасывает пулю назад. Для защиты лучше использовать углеродные нанотрубки с толщиной стенок в один атом, но, по возможности, с большим диаметром.

По оценкам ученых, для легкого бронежилета, способного выдержать пистолетный выстрел с типичной энергией пули в 320 джоулей, достаточно шести слоев ткани, свитой из нанотрубок толщиной по 100 мкм. И пули от такого бронежилета толщиной меньше миллиметра будут буквально отскакивать - ему не страшны даже несколько выстрелов подряд в одно и то же место. Это выгодно отличает гипотетический бронежилет от современных аналогов из кевлара или других материалов. В них пули застревают, а бронежилет портится, распределяя энергию пули на большую площадь, так что хороший синяк или даже поражение внутренних органов от удара обеспечены. Конечно, синяков и в новом бронежилете не избежать, но лучше уж синяк, чем дырка в теле. Теперь дело за малым - изготовить углеродный бронежилет на практике. Поскольку технология прядения нитей из нанотрубок уже отработана, принципиальных трудностей тут вроде бы не предвидится. ГА

Мелкий бас

Новый наполнитель для громкоговорителей, позволяющий существенно улучшить их отдачу на басах, разработали инженеры корпорации Matsushita Electric Industrial, в миру больше известной под торговой маркой Panasonic. Углеродные частички с нанопорами эффективно адсорбируют лишний воздух при повышении давления за динамиком и позволяют при прочих равных вдвое уменьшить объем корпуса.

Улучшение качества баса всегда было головной болью разработчиков акустических систем. Именно на басах труднее всего добиться малых нелинейных искажений, причем нижняя

воспроизводимая частота определяется, по сути, объемом громкоговорителя. А с доступным объемом становится все хуже и хуже - прогресс бытовой техники диктует необходимость миниатюризации. За последние семь лет сотовые телефоны похудели вдвое, а телевизоры стали тоньше в шесть раз. Даже с нормальным воспроизведением голоса, частотный диапазон которого начинается с трехсот герц, в тонких устройствах уже возникают большие проблемы. А что будет со звуком дальше, если эта тенденция сохранится?

У любого громкоговорителя, как у грузика на пружинке, есть собственная резонансная частота колебаний, ниже которой его эффективность быстро падает. Чтобы эту частоту понизить, нужно либо увеличивать массу диффузора, что снижает отдачу, либо делать более мягким подвес. Но каким бы мягким подвес ни сделали, воздух за диффузором будет при сжатии или расширении играть роль пружины, повышая резонансную частоту.

Чтобы уменьшить негативное влияние воздуха, используют различные наполнители. Сначала применяли вату или шерсть, потом синтетические волокнистые материалы. Обычно их считают звукопоглотителями, но на самом деле их роль совсем в другом. Воздух при сжатии нагревается, и если тепло эффективно поглощать (что и делают волокна ваты или синтетики), то сжиматься он будет легче. При расширении все происходит в точности наоборот. Таким способом эффективный объем громкоговорителя можно увеличить в лучшем случае на тридцать процентов, и этот предел не зависит от конструкции и определяется лишь термодинамическими свойствами воздуха.

Предлагалось и множество других способов обойти упругость воздуха. Например, можно сделать объем за диффузором герметичным и заполнить его подходящим веществом вблизи температуры кипения, которое будет эффективно конденсироваться при уменьшении объема и испаряться при увеличении. Или попытаться подобрать смесь паров так, чтобы ее свойства были похожи на свойства вещества в так называемой критической точке, в которой стирается грань между газом и жидкостью и сжимаемость стремится к бесконечности. Однако все эти способы не лишены серьезных недостатков, слишком сложны в реализации и распространения пока не получили.

Инженеры Matsushita решили использовать другое явление - адсорбцию молекул поверхностью. Для этого были получены частички углерода размером не более ста микрон с развитой системой пор порядка нескольких десятков нанометров поперечником. Большая поверхность нанопор эффективно адсорбирует воздух при сжатии, снижая его упругость.

Утверждается, что оптимальные размеры и параметры пористости частичек позволяют либо уменьшить объем громкоговорителя (как говорилось выше, в два раза), либо - при неизменном объеме - уменьшить нижнюю частоту со 120 до 80 Гц динамика телевизора и с 1200 до 800 Гц у компактного сотового телефона.

В плоских телевизионных панелях, кроме того, оказалось удобным использование так называемого пассивного радиатора - еще одного плоского динамика без магнитной катушки. Пассивный радиатор, как и более популярный фазоинвертор, трубу которого просто негде разместить в тонкой телевизионной панели, создает еще один акустический резонанс конструкции ниже резонансной частоты динамика и таким способом способствует лучшей передаче баса.

Разработчики утверждают, что углеродные частички с нанопорами улучшают не только бас. Увеличение эффективного объема благотворно сказывается и на средних частотах вплоть до двух килогерц. Matsushita планирует использовать новую технологию в широком спектре продукции: первыми на очереди стоят плазменные телевизоры. ГА

Новости подготовили

Галактион Андреев
Александр Бумагин
Евгений Васильев
Владимир Головин
Евгений Гордеев
Артем Захаров
Евгений Золотов
Сергей Кириенко
Денис Коновальчик
Игорь Куксов
Алексей Носов
Павел Протасов
Иван Прохоров
Дмитрий Шабанов

Микрофишки

Австралийский исследователь Джон Папандриопулос (John Papandri-opoulos) утверждает, что разработал технологию, позволяющую в несколько раз повысить скорость передачи данных в DSL-соединениях. Их пропускную способность во многом ограничивает перекрестная интерференция, возникающая между кабелями: Папандриопулос предлагает решить проблему за счет специальных методов оптимизации и регулировки мощности сигналов. Внедрение системы, видимо, потребует установки на стороне провайдера нового оборудования, а клиентские модемы можно будет просто "перепрошить". Профессор Стэнфордского университета Джон Сиоффи (John Cioffi), которого называют "отцом DSL", так впечатлился результатами Папандриопулоса, что предложил 29-летнему ученому работу в своей компании ASSIA. ВГ

***

Инструмент для мобильного браузинга Opera Mini обновился до четвертой версии. Программа-клиент была полностью переписана, что позволило нарастить функциональность, сохранив скромный размер дистрибутива (не более сотни килобайт).

В списке нововведений выделяются два пункта. Во-первых, улучшенный режим рендеринга, представляющий веб-страницу в виде миниатюры, с возможностью увеличения отдельных участков. Эта фича более требовательна к трафику, нежели компиляция данных в одну колонку, как было раньше, но и в этом

случае компрессия достигает порой нескольких сотен процентов, что порадует экономного пользователя. Во-вторых - поддержка платформы Opera Link, нового сервиса в составе портала MyOpera. Служба позволяет синхронизировать закладки между настольным (начиная с версии 9.5, пока пребывающей в статусе беты) и мобильным браузерами. Из приятных мелочей отметим возможность переключить экран в альбомный режим.

Opera Mini еще не исчерпала резервы для совершенствования. Например, ресурсы, функциональность которых завязана на технологии AJAX, скорее всего окажутся неработоспособны. Та же участь постигнет сайты, над которыми трудились недальновидные дизайнеры, использующие Flash-элементы для навигации. А3

Босс есть босс

Автор: Александр Бумагин

Третьего ноября в США завершился третий конкурс DARPA среди автомобилей-роботов. В отличие от не очень удачных космических состязаний, поддерживаемых правительством США, DARPA Grand Challenge олицетворяет собою технический прогресс во всей его красе. Во всяком случае, уже второй раз подряд к финишу конкурсной дистанции добирается больше одного автомобиля, а приготовленные денежные призы не залеживаются.

Организатором конкурса является Пентагон, а точнее, входящее в это ведомство Агентство передовых оборонных разработок (Defense Advanced Research Projects Agency, DARPA). Реверанс в сторону космоса в предыдущем абзаце был не случайным: DARPA образовалось в 1958 году, и это было ответом на запуск в СССР первого спутника. Таким образом, с некоторой натяжкой можно считать, что Интернет, зародившийся в недрах именно этой организации, тоже обязан своему появлению начавшейся космической гонке.

Но вернемся с небес на землю. В DARPA Grand Challenge участвуют автомобили, переделанные командами из разных университетов мира, а главное и, можно сказать, единственное умение, которым должны обладать конкурсанты, это полная автономность в дорожных условиях. Никакого дистанционного управления. Все решения по конкретной ситуации машина должна уметь принимать на месте самостоятельно.

Разумеется, цель, преследуемая DARPA при проведении мероприятий подобного рода, далека от благотворительности. Существует многолетняя программа, согласно которой к 2015 году около трети всех автомобилей, состоящих на службе

Пентагона, планируется заменить роботами, дабы уменьшить потери личного состава в вооруженных конфликтах. От умения самостоятельно ездить по бездорожью до способности выбирать и поражать цель - один шаг, а потому ассоциации со знаменитой трилогией о Терминаторе приходят на ум не случайно. Подобные сравнения находят уместными не только журналисты. Например, одна из команд-участниц DARPA Grand Challenge так прямо и назвала своего "питомца" - SkyNet, по имени взбесившегося суперкомпьютера из упомянутого киношедевра.

А начиналось все, напомним, в марте 2004-го в окрестностях калифорнийского города Барстоу. Там же, по сути, все и завершилось: первый блин вышел комом. Лучшая из машин-участниц первого конкурса прошла лишь пять процентов всей дистанции. Маршрут длиной 230 км был проложен по пересеченной местности, а основная задача сенсоров и бортовых программ состояла в правильной реакции на неподвижные объекты - особенности местности и рельефа. Неизвестно, присущ ли автомобилям-роботам предстартовый мандраж, но тогда, в 2004-м, семь из пятнадцати машин даже не сумели покинуть стартовую зону.

В октябре 2005 года на старт пустынной трассы в Мохаве вышли уже 23 команды, но 18 из них к финишу даже не приблизились. Грузовик TerraMax сумел преодолеть дистанцию, но не уложился в отведенные на это 10 часов. Главное же достижение DARPA Grand Challenge состояло в том, что целых четыре автомобиля справились с пустыней в срок, а победил с результатом 6 часов 54 минуты Volkswagen Touareg Стэнфордского университета, опередивший ближайшего преследователя на 11 минут. Стэнфордской команде прочили победу и в этом году.

Спонсорская интуиция

Среди автомобильных марок роботов-финалистов наибольшее представительство имели Volkswagen (три Passat'a), Ford (пикап F-250 и гибридный Escape), а также Chevrolet (два внедорожника Tahoe). Все прочие - Subaru, Toyota, LandRover и Oshkosh - выступали поодиночке. Победителем же в этом неофициальном зачете производителей следует считать брэнд Chevrolet. Оба автомобиля этой марки закончили соревнования в срок, а один их них даже выиграл Urban Challenge.

Любопытна также прозорливость спонсоров: Intel и Google вместе помогали командам, занявшим первое и второе места. Впрочем, выбор технологических гигантов вполне объясним. Команда из Карнеги-Меллона была фаворитом самых первых гонок благодаря огромному опыту ее руководителя Уильяма Уиттекера (William Whittaker). В 2005-м из-за досадных технических проблем у питсбургцев победа уплыла в руки Стэнфордской команды (кстати, ее руководитель Себастьян Трун [Sebastian Thrun] - бывший ученик Уиттекера). Говорят, тогда в Карнеги-Меллоне с горя повесили на стену фотографию машины из Стэнфорда и метали в нее дротики. И вот теперь флюгер переменчивой фортуны вновь совершил поворот.

Легкой жизни, правда, организаторы никому не готовили. В DARPA вовсе не собирались отдавать еще 3,5 млн. долларов призовых денег за одни и те же достижения. Действие перенесли из пустыни в городские условия, а нынешний конкурс получил название Urban Challenge. Команды должны были привить своим роботам правила хорошего тона, научив их ездить по улицам, с учетом дорожной разметки и разнообразных препятствий, в том числе и движущихся (причем от машин требовалось "хорошее зрение" не только у себя под носом, но и вокруг на расстоянии до двухсот метров). Автомобили в обязательном порядке должны были уметь обгонять, совершать повороты и развороты, в нужном месте останавливаться на перекрестке, даже парковаться, и все это - не нарушая правил дорожного движения - их свод был одним из основополагающих документов конкурса. Городской маршрут протяженностью 96,5 км нужно было проехать за шесть часов. Дистанция делилась на три участка, на которых проверялись различные элементы обязательной программы.

Из 89 поданных заявок судьи отобрали для квалификационных заездов лишь 35 команд, причем 24 отсеялись в ходе проверок. Так что на старт Urban Challenge выехали лишь 11 машин-роботов. В прошлом конкурсе схема пути за два часа до старта была предоставлена командам на компакт-диске. Прогресс

затронул и эту сторону гонок: на сей раз за те же два часа до начала маршрут скопировали в бортовой компьютер каждого автомобиля с флэш-карты. По всему пути были расположены контрольные точки, над которыми в нужном порядке должен был проследовать передний бампер каждой машины. В итоге все эти нюансы сказались на распределении призовых мест: выиграл вовсе не тот автомобиль, который финишировал первым, а тот, движение которого полностью соответствовало дорожным правилам.

Нужно подчеркнуть, что стартовали машины не одновременно, а одна за другой с некоторым интервалом. Кроме того, движение не было непрерывным: организаторы принудительно останавливали каждый автомобиль по своему усмотрению - в частности, для того, чтобы в некоторых местах трассы участники не мешали друг другу. По этой причине борьбы на финише быть и не могло: для каждого участника работал свой секундомер.

Через час после старта с трассы сошли четыре автомобиля, при этом две машины умудрились столкнуться со зданиями. Одно из строений почти протаранил тот самый грузовик TerraMax, героически доползший до финиша в прошлый раз. Позднее из гонки выбыл еще один робот. Неприятная ситуация возникла между автомобилями SkyNet и Talos, которые, не разобравшись в дорожной ситуации, слегка задели друг друга, но оба остались в строю и сумели закончить состязания, хотя уже и не могли претендовать на призовые места.

К концу соревнований стало ясно, что на первый приз в два миллиона имеются три претендента: автомобиль Junior Стэнфордского университета, Odin из Виргинского технологического и Boss из Университета Карнеги-Меллона. Хронологически первым пересек финишную ленту Junior, однако

повторить триумф Стэнфорду было не суждено: уступив победителю в средней скорости всего 1,5 км/час, Junior оказался вторым с отставанием около двадцати минут. Еще столько же проиграл Odin, в итоговой табели о рангах он - третий. Ну а первым стал Boss со своей командой Tartan Racing Team. Boss двигался в среднем быстрее (22,5 км/час) и аккуратнее конкурентов. Забавно, что телевизионная аппаратура одной из компаний своими радиопомехами чуть не сорвала старт будущего победителя, но, слава богу, за четверть часа неполадки удалось исправить.

Кроме денег спонсоров, Босса привели к победе 27 датчиков и камер, установленных на машине, десять "блэйдов" на Intel Core 2 Duo 2,16 ГГц, 500 тысяч строк машинного кода и, конечно же, огромная команда инженеров, программистов и тестеров. Система ориентации в пространстве была настроена так, что одно и то же направление в каждый момент времени контролировало как минимум два датчика, обеспечивая необходимую избыточность информации. Десятки раз в секунду управляющее программное обеспечение создавало модель окружающей среды и на основе этой модели принимало нужное решение.

Конечно, это только первый шаг к фантастике в виде беспилотных танков и такси (на выбор). Скорость в 22,5 км/час даже для запруженной пробками Москвы выглядит смешной, к тому же значительная часть возможностей, продемонстрированных роботами-автомобилями, была связана с идеальной дорожной разметкой, этим неизменным атрибутом американских дорог. Неизвестно, как бы закончился конкурс, проводись он в условиях, приближенных к средним по России. После окончания соревнований организаторы DARPA Grand Challenge, разумеется, лучились оптимизмом. По их оценкам, через десять лет роботы и впрямь будут разъезжать по городам. Надеемся, что это будут не роботы-полицейские.

А пока технике очень даже есть куда расти. Отчего бы, скажем, DARPA не устроить в будущем автопробег роботов через все Соединенные Штаты, от побережья к побережью? При этом можно сделать обязательными такие умения, как устранение прокола шины и установка запаски, пользование бензоколонками и автосервисом, а также уплата штрафа за превышение скорости.

Что касается автомобиля с пугающим названием SkyNet, то из финишировавшей в Urban Challenge шестерки он пришел последним. Если это событие и является знаковым, то не вполне ясно, на каком слове делать акцент: "пришел" или "последний"?

Шутка шуткой…

Даже безоружные роботы вызывали определенные опасения у организаторов. Дабы держать руку на пульсе (точнее, на рубильнике), командам-участницам требовалось обеспечить свой автомобиль беспроводным интерфейсом, по которому можно было бы передать команду о немедленной остановке. Самим участникам, разумеется, использовать этот управляющий канал было нельзя, а вот судьи не раз и не два к этому средству прибегали.

Кроме того, курьезным показалось обращение одного из организаторов к публике, собравшейся в стартовой зоне. Он попросил по возможности, на всякий случай, выключить мобильные телефоны. Мало ли…

Естественные процессы

Автор: Илья Щуров Voyager

В широком потоке ежедневных ИТ-новостей подавляющая доля известий, ясное дело, приходится на уже привычную текучку: новые версии известных устройств и программ, чуть более быстрые чипы, еще более емкая память и т. д. В области защиты информации, однако, ситуация иная: естественные процессы развития тут постоянно не соответствуют ожиданиям. Иначе говоря, воспринимаются как противоестественные. Если неуклонный рост быстродействия процессоров и вместимости накопителей информации устраивает всех, то невозможность защитить информацию от копирования флагманы индустрии считают не просто заблуждением, а вредной и опасной ересью. Что же касается защиты систем от вирусов, то здесь новости вроде бы должны приносить известия об общем росте безопасности, однако на самом деле сообщают лишь о том, что ситуация, по сути дела, не меняется.

В конце октября небольшая, но знаменитая фирма SlySoft с карибского острова Антигуа выпустила пресс-релиз, замеченный практически всеми, кто интересуется оптодисками с видео высокой четкости. Официально запрещенные в США и большинстве стран Европы, программы SlySoft AnyDVD и CloneDVD давно известны как удобное средство для резервного копирования DVD-фильмов. Или как один из главных инструментов пиратства, если смотреть с другой стороны. В начале 2007 года программа AnyDVD HD стала первым на рынке коммерческим продуктом, обеспечивающим качественное копирование контента с дисков высокой четкости в форматах HD DVD и Blu-ray. В течение года технология AACS, защищающая контент на этих дисках от копирования, подвергалась неоднократным модификациям. И вот теперь новый пресс-релиз SlySoft известил пользователей о том, что успешно взломана последняя версия защиты AACS Media Key Block v4. Иными словами, выпущена очередная версия программы AnyDVD 6.1.9.3, без проблем копирующая контент со всех HD-дисков, защищенных всеми версиями AACS вплоть до последней.

Но что еще интереснее, в этом же пресс-релизе сообщается, что фирмой уже взломана и "суперзащита" BD+, реализованная пока лишь в некоторых новых видеофильмах на дисках Blu-ray. В настоящее время, по словам главы разработчиков SlySoft Джеймса Вонга (James Wong), технология снятия защиты BD+ доводится до товарного вида и до конца текущего года будет добавлена в

AnyDVD HD. А это означает, что падет последний бастион "невскрываемой защиты" HD-видео, и киноиндустрия, возможно, все же начнет осознавать недостижимость победы в этом состязании.

Другая созвучная новость, появившаяся аккурат в Хэллоуин, сильно огорчила поклонников Apple, привыкших считать, что Mac-платформа в силу своей замечательной природы более безопасна, чем все остальные. Хотя эксперты по защите информации всегда подчеркивали, что почти нулевая распространенность вредоносных кодов для Маков - лишь следствие небольшой доли яблочных компьютеров в общей массе. Но если популярность системы Apple начнет расти, предупреждали специалисты, тут же станут плодиться и всякие вирусы-черви. Что, собственно, и происходит ныне (существовавшие до сих пор фруктовые вредители были не особенно опасны и представляли собой скорее демонстрационные концепты). Последние годы были для Mac-платформы довольно благополучными: число пользователей быстро росло, отчасти на волне успеха iPod и iPhone. А потому вопрос о компьютерной заразе для Apple из категории "если" сам собой перешел в "когда".

Теперь же известен и ответ на данный вопрос - начиная с Хэллоуина 2007 года. В эти дни сразу на нескольких порнографических сайтах появился троянец, заточенный под платформу Mac и получивший название OSX.RSPlug. Программа маскируется под плагин для плеера Quicktime и предлагает себя установить для просмотра видеороликов, представленных на сайтах кадрами-фотографиями. Учитывая, что ранее эти порносайты активно рекламировались в спаме и на веб-форумах, многие откликнувшиеся на приглашение пользователи соглашались на установку "плагина" - и получали троянца-шпиона, подменяющего DNS-адреса, ворующего информацию и, как показала проверка, не выявляющегося ни одной из трех десятков антивирусных программ для Маков. Ситуацию, конечно, быстро исправили, но ясно, что первая ласточка прилетела.

Не порадовала с точки зрения безопасности и новейшая версия операционной системы Mac OS X Leopard, создававшаяся, по словам Apple, с упором на укрепление защиты. Как показало тестирование германского ИТ-издания Heise, встроенный брандмауэр "Леопарда" оказался откровенно плох. Вердикт по итогам независимой проверки выглядит так: "Файрволл системы Mac OS X Leopard провалил все тесты. Он не активизируется по умолчанию (более того, уже работающий файрволл при апгрейде отключается), а когда активирован, то не работает как положено. И даже при самых жестких установках параметров (блокировать

все входящие подключения) он все равно позволяет доступ к системным службам из Интернета (в частности, не отключается внешнее управление функциями NetBIOS)". Наконец, помимо брандмауэра в Leopard включены старые версии сторонних программ, для которых уже известны и устранены дыры в безопасности. В целом же, заключают эксперты, "в вопросах безопасности Apple демонстрирует бессистемный подход, сильно напоминающий то, что делала Microsoft четыре года назад". Критический материал Heise достаточно подробен в деталях, которые здесь перечислять вряд ли уместно, коль скоро в Сети доступен оригинал (www.heise-security.co.uk/articles/98120). Но одну деталь все же надо подчеркнуть. С точки зрения (не)безопасности платформа Windows в свое время стала жертвой собственной беспрецедентной популярности. Та же судьба, похоже, ожидает Mac OS.

тема номера: Всепроникающая небезопасность

Автор: Илья Щуров Voyager

Занимаясь подготовкой сегодняшней темы номера, я стал форменным параноиком, а проникновение информационных технологий буквально в каждый уголок жизни начало казаться угрозой нашей цивилизации пострашнее ядерной зимы и глобального потепления вместе взятых. Конечно, это некоторое преувеличение, но... Судите сами.

ЦИФРЫ

Один из первых троянцев, созданных для захвата данных из банковских форм (Bebrew), действовал необнаруженным в течение девяти месяцев и собрал при этом около 113 Гбайт данных.

По данным cio.com со ссылкой на Secure Science Corp

Если вы - "простой пользователь", то ваш компьютер находится под угрозой. Скорее всего у вас нет антивируса (а если есть - то с истекшей лицензией и устаревшими базами), файрволла (а если есть - вы не знаете, как с ним работать, и разрешаете все соединения), а операционка не обновлялась уже много лет.

Если вы - "продвинутый пользователь", заботящийся о своей безопасности, у вас есть антивирус, файрволл и вы честно ставите все заплатки для Windows, как только она этого попросит - ваш компьютер находится под угрозой. Скорее всего вы забыли обновить какую-нибудь из ваших многочисленных любимых программ, а в ней недавно обнаружилась большая и страшная дыра, через которую рано или поздно полезет какая-нибудь нечисть.

Наконец, если вы - форменный параноик, каковым за последние две недели стал и я, у вас всегда самые свежие версии всех программ и антивирусных баз, вы помните наизусть все номера открытых и закрытых портов вашего файрволла - ваш компьютер все равно под угрозой. Ибо никто вас не защитит от "zero-day" (0day) атак - когда новая дырка в безопасности обнаруживается и используется злоумышленниками раньше, чем о ней успевают узнать (и, следовательно, залатать) разработчики. Возможно, речь идет о нескольких часах или днях (а иногда - и

месяцах), но даже получив доступ к компьютеру на несколько минут, можно натворить бед.

Компьютеры ужасающе небезопасны, и это аксиома. Но компьютеры повсюду. С одной стороны, мы все больше переносим свою деятельность в Интернет. Наша "вторая жизнь" проходит там целиком, "первая" же - сильно от него зависит. С другой - нас окружает множество самых разных устройств с процессорами, большинство из которых может выполнять произвольный код - а значит, является уязвимым.

А там, где есть уязвимость, появится и злоумышленник. Новые технологии порождают новые виды угроз, а компьютерная преступность меняется количественно и качественно, становясь настоящей индустрией. Противостоящая ей индустрия - в первую очередь та ее часть, которая по традиции называется антивирусной, - эволюционирует медленно и, кажется, не очень охотно: предлагая скорее экстенсивный путь развития ("еще быстрее! еще больше!"), нежели какие-то подходы к принципиальному решению проблем. Борьба щита и меча продолжается. И щит, и меч - в выигрыше; в проигрыше все остальные.

Эта ситуация заставляет задуматься над фундаментальным вопросом устойчивости нашей цивилизации. Взгляд, представленный в теме, кажется довольно мрачным даже мне самому: мы будем говорить о том, что есть объективные экономические причины текущего плачевного состояния дел в сфере безопасности, а значит, изменить ситуацию только техническими средствами нельзя. Причины кроются не в технологиях, а в людях; технологии лишь позволили этим причинам проявиться. Но как тогда быть? Мы хорошо (пожалуй, слишком хорошо) знаем, что любая попытка воспитать "нового человека" обречена на неудачу. Надежда на то, что грядущие поколения будут относиться к безопасности компьютерных систем не так, как мы, довольно призрачна.

Одна из ключевых проблем состоит в том, что безопасность является общественным благом, и чтобы эффективно им распоряжаться, люди должны уметь договариваться друг с другом. История показывает, что в принципе это возможно: например, используя общие дороги, мы ездим по правой стороне, и даже иногда соблюдаем правила дорожного движения. Однако большинство договоренностей носит локальный характер, и их действие в лучшем случае ограничено масштабами одного государства, - в Англии и Японии люди ездят по левой стороне и горя не знают.

Проблема безопасности Интернета носит глобальный

характер - и этим она похожа на проблему экологии или мирового терроризма. Ни одна из них в данный момент не решена.

Существует ли "инстинкт самосохранения" у человечества как целого? Может ли этот инстинкт взять верх над личной выгодой "здесь и сейчас"? Вряд ли мы скоро получим ответы на эти вопросы: цивилизация никогда не была столь глобальной, и у нас нет исторического опыта, на основе которого можно бы делать какие-то выводы. Но именно от ответов на них зависит, возникнут ли общественные институты, которые смогут эффективно решать такие проблемы.

Впрочем, может быть, все не так уж и мрачно. Наверное, со временем мы привыкнем не доверять программируемой технике. Расплачиваться будем наличными, пароли записывать на бумажках, важные письма отправлять обычной почтой.

Приспособимся, в общем. Мир перестанет быть глобальным, и все будет как раньше. Должно же что-то затормозить экспоненциальный рост прогресса, наблюдаемый последние несколько десятков лет?

Экономика без опасности

Автор: Илья Щуров Voyager

Можно долго говорить о противостоянии технологий "нападения" и "защиты" в информационной безопасности, но на самом деле речь всегда идет о противостоянии людей. Вредоносное ПО и антивирусы не борются друг с другом - они лишь делают то, для чего предназначены. И проблемы, связанные с ИБ, не только технические, но и во многом социальные, требуют анализа и поиска способов решения.

Нарисованная дверь

ДОСЬЕ

Предположительно штат 76service состоял из двух человек: один из них россиянин, скрывавшийся под ником 76, другой звался Exoric и был из Мексики. 76 занимался собственно кодом троянца, а Exoric разрабатывал веб-интерфейс.

Представители антивирусных компаний не устают напоминать журналистам и пользователям, что противостоят не кучке студентов-вирусописателей, занимающихся самоутверждением, а мощной преступной индустрии, в которой задействовано множество людей и крутятся немалые деньги и которая, в свою очередь, противостоит антивирусным компаниям. Дело поставлено на поток, объем вредоносного ПО растет как снежный ком, а в арсенале вирусописателей появляются все новые и новые технологии. "Количество записей в антивирусной базе каждый год примерно удваивается", - говорит Виталий Камлюк, старший вирусный аналитик "Лаборатории Касперского", - и это еще довольно осторожная оценка. Однако важны не только количественные, но и качественные характеристики эволюции мира компьютерной преступности. Сейчас он представляет собой сложную структуру, в которой собственно разработчики зловредного ПО - лишь одно из звеньев.

Исследователю из компании SecureWorks Дону Джексону (Don Jackson) удалось заглянуть в мир современного malware практически изнутри. Все началось в январе 2007 года, когда один знакомый попросил Дона посмотреть на странную "экзешку", непонятно как появившуюся на его компьютере. Файл

(Джексон назвал его Gozi [Вообще-то, поначалу он назвал его pesdato (это слово встречается в коде), но когда узнал, что оно означает по-русски, переименовал открытие]), оказался неизвестным на тот момент антивирусной науке (то есть zero-day) трояном, который перехватывал персональные данные, вводимые пользователем в веб-форме при работе с системами онлайн-банкинга. Потратив несколько дней на изучение "неведомой зверюшки", Джексон вышел на сайт 76service.com, встретивший его лаконичной формой для ввода логина и пароля. Это была словно нарисованная на холсте дверь, ведущая в неведомый мир владельцев Gozi.

Изучая форумы кардеров, Джексон наткнулся на группу HangUp Team (предположтельно располагающуюся в Архангельске), которая имела какое-то отношение к Gozi и 76service. Сделав несколько неудачных попыток получить тестовый доступ к сервису (провалившихся во многом из-за незнания русского языка), Джексон, в конце концов, раздобыл заветный "золотой ключик" через своего знакомого, расследовавшего деятельность HangUp Team. Дверь открылась.

Комментарий

Из беседы с Виталием Камлюком, старшим вирусным аналитиком "Лаборатории Касперского".

Не возникнет ли ситуация, при которой мне придется тратить 99% ресурсов своего компьютера на работу антивируса и 99% трафика на обновление его баз?

- Сейчас обновления не столь большие. Антивирусные записи хранятся компактно, они не содержат в себе мегабайты кода. Движок построен так, что значительный рост числа записей не сильно влияет на скорость работы движка. База может быть гигантской, она может быть в сто раз больше, и скорость упадет незначительно.

То есть у этой технологии есть запас - скажем, лет на пять?

- Я думаю, что на больший срок. Проблема в другом: как справляться с этим потоком? Штат компании не может расти экспоненциально. Мы и не растем, это проигрышная стратегия - расти вслед за вирусным кодом. Мы разрабатываем технологии, которые позволяют обрабатывать весь этот вирусный поток. В ответ на автоматизацию процесса написания вирусов у нас есть своя автоматизация. Трояны сходят с "конвейера", мы их аккуратненько поднимаем и переносим на наш конвейер, где

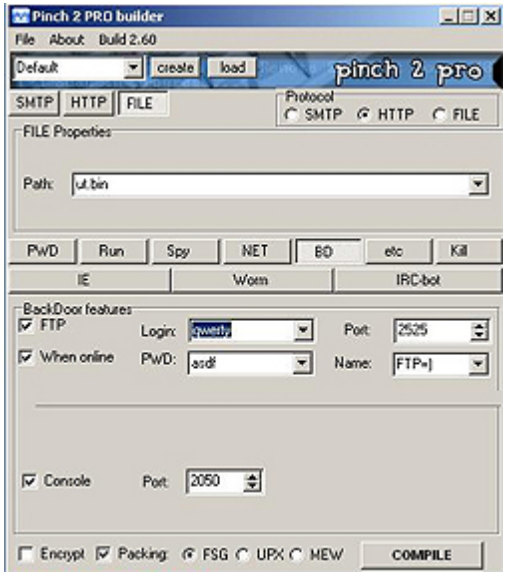
автоматически детектируем, не задействуя человеческие ресурсы.

Это понятно, но ломать не строить: запутывать код проще, чем распутывать, и т. д. Вы будете на шаг позади…

- Нам просто нужно работать эффективнее, быть гораздо сильнее и умнее, чем они. У нас разные уровни: у вирусописателей технический уровень может быть ниже, чем у вирусного аналитика. Так или иначе, это подпольное предприятие, и все понимают, что оно временное. Там все-таки нет уверенности, как у настоящей индустрии, хотя мы и называем ее так из-за масштабов и довольно сложной структуры.

Malware as a service

Увиденное за дверью стало для Джексона полной неожиданностью. Gozi оказался не внутренней разработкой взломщиков, созданной для своих нужд. Не предназначался троян и для продажи. Он был основой сервиса, своеобразного криминального магазина самообслуживания. Пользователь системы, имеющий аккаунт, мог подписаться на доступ в течение месяца к информации, поступающей с каких-то Gozi-инфицированных машин по цене от $1000 за штуку. Войдя в систему, пользователь видел список "своих" троянов и мог анализировать полученные от них "передачи". Насколько удачным оказывался "улов" и как клиент преобразовывал украденные данные в деньги - было уже проблемой подписчика. Чаще всего подписчики продавали добытые сведения на черном рынке тем людям, которые непосредственно занимались снятием денег со счетов и покупкой товаров, и реже использовали эти сведения самостоятельно.



Владельцы 76service этим не занимались - точнее, могли не заниматься. Они в первую очередь предоставляли сервис и делали все на благо своих клиентов. Помимо базового комплекта, за небольшую плату они могли провести дополнительный анализ и просеивание информации - например, отобрать из всех поступающих данных только те, которые относились к клиентам определенного банка.

Все как в "большом мире". Не единичные "спецоперации" - атаки и взлом компьютеров, - а хорошо отлаженный механизм, конвейер и готовое "решение" (выражаясь современным бизнес-языком), допускающее четкое разделение труда и создание длинных цепочек потребления. На примере Gozi и 76service мы видим развитие теневой экономики malware. Борьба с киберпреступностью будет неэффективна до тех пор, пока не будут учитываться свойства этой экономики.

В настоящий момент сайт 76service.com не открывается, а троян Gozi детектируется основными антивирусами. Но это трудно назвать победой: в середине марта 2007 сайт тоже на время закрывался, но спустя буквально несколько дней он появился вновь, переехав на хостинг где-то в Гонконге и выпустив новую версию трояна. Вполне вероятно, что сейчас функционирует аналогичный сервис, работающий на другом домене и использующий очередную модификацию трояна, сигнатура которого еще не добралась до антивирусных баз. Может быть, он перехватывает данные и с вашего компьютера всякий раз, когда вы вводите свой платежный пароль в Яндексе.

Тараканьи бега

Для простоты, будем считать, что какой-то большой и сложный продукт - например, Windows 2000 - содержит 1 миллион ошибок, причем каждая ошибка "проявляется" в среднем раз в 1 миллиард часов. Предположим, что Падди работает на Ирландскую Республиканскую армию и его задача - взломать компьютер Британской армии, чтобы получить список информаторов в Белфасте; задача Брайана - остановить Падди. Чтобы это сделать, ему нужно узнать об ошибках первым.

Падди работает в одиночку и может потратить на тестирование только тысячу часов в год. У Брайана есть доступ к полному исходному коду Windows, десятки кандидатов наук в подчинении, контроль за исследовательскими коммерческими компаниями, прямой доступ к CERT и соглашение об обмене информацией с компетентными службами Англии и США. Кроме того, он имеет возможность посылать консультантов на стратегически важные объекты (например, в сфере энергетики и телекоммуникаций), дабы объяснять сотрудникам этих объектов, как им лучше защищать свои системы. Допустим, что Брайан и его подчиненные тратят в общей сложности 10 миллионов часов в год на тестирование.

Через год Падди найдет одну ошибку, тогда как Брайан найдет сто тысяч. Однако вероятность того, что Брайан нашел ту же ошибку, что и Падди, равна 10%. Через десять лет он найдет ее - но за это время Падди найдет еще девять, и вряд ли Брайан будет к тому моменту знать их все. Более того: отчеты Брайана об ошибках станут литься таким потоком, что Microsoft просто перестанет обращать на них внимание.

Ross Anderson, "Why Information Security is Hard - An Economic Perspective"

Сделай сам

История 76service - лишь эпизод, показывающий, как сейчас выглядит индустрия malware. Другой тревожный сигнал - появление множества "наборов юного взломщика" и конструкторов "сделай троянца своими руками". Подобные приложения позволяют легким движением руки комбинировать последние достижения передовой мысли компьютерного андеграунда, создавая уникальные средства заражения. В качестве примера можно привести MPack - набор серверных скриптов (классическая связка PHP + MySQL) с дружественным

интерфейсом и удобной системой администрирования, позволяющий проникать в компьютер жертвы и устанавливать на нем вредоносное ПО с помощью одного из множества эксплойтов в популярных программах, а также через iframe-дыры на сайтах. Как и положено, программа умеет автоматически обновлять свои базы дыр. Вам это ничего не напоминает? По данным PandaLabs на лето этого года, стоит такая игрушка около тысячи долларов - не слишком высокая цена за подобное чудо технической мысли.

"Продолжающаяся разработка MPack свидетельствует о том, что преступники вовсю используют преимущества онлайнового мира для получения прибыли, - пишет исследователь компании Symantec Хон Ло (Hon Lau) в корпоративном блоге. - В компьютерной преступности риск быть пойманным очень мал; еще меньше риск физической опасности… Поэтому неудивительно, что новые типы атак и апдейты к существующим продолжают появляться".

Есть и гораздо более дешевые решения - 20–40 долларов за штучку (TrafficPro). Есть конструкторы (такие как Pinch), позволяющие с помощью интуитивно понятного интерфейса настроить все параметры будущего трояна (протокол обратной связи, способ автозапуска, вид деятельности, метод кодирования, необходимость отключения антивирусного ПО и т. д.). Есть удобные системы, позволяющие рассылать спам и заражать форумы, работающие на самых разных движках.

Порог вхождения в индустрию компьютерной преступности снизился до минимума. Открытые форумы взломщиков можно найти с помощью Google, а чтобы выйти на виртуальную "большую дорогу" и начать "зарабатывать" реальные деньги, достаточно иметь несколько десятков долларов стартового капитала. В то же время техническое оснащение взломщиков вполне сопоставимо с техническим оснащением антивирусных компаний.

Опасная глобальность

Процветание и устойчивость экономики компьютерной преступности обусловлены рядом причин, порой уникальных. Редактор CSO Magazine Скотт Беринато говорит о проблеме "распределенного ущерба" (distributed pain): если украсть у миллиона людей по одному доллару, скорее всего никто из них этого даже не заметит - и уж точно не станет вызывать полицию и писать жалобы, даже если "ограбление" происходит с регулярностью раз в месяц. А современные глобальные

технологии позволяют делать именно это. Примерно той же позиции придерживаются многие банки - защищая свои системы настолько, насколько этого требует законодательство, они готовы списывать периодические потери от киберпреступности на "допустимые издержки" (закладывая их, естественно, в стоимость своих услуг, процентные ставки и т. д.).

"Аналогичная ситуация с правоохранительными органами, - Скотт цитирует Джима Малони (Jim Maloney), бывшего CSO Amazon.com, в настоящий момент - владельца собственный консалтинговой компании. - До тех пор, пока не поступит достаточно информации от множества жертв и не станет ясно, что речь идет об одной большой проблеме, необходимых для ее решения ресурсов просто никто не выделит".

С другой стороны, распределенная структура преступных корпораций и длинные "цепочки потребления" позволяют "размазывать" риски по всем участникам этого рынка - точно так же, как в наркобизнесе. Разделение труда приводит к повышению устойчивости всей системы. Для наркомафии арест одного наркокурьера - все равно что слону дробинка. Так и арест одного разработчика трояна не затронет "клиентов" его сервиса, и через какое-то время аналогичный сервис появится в другом месте и с участием других людей.

Враг государства

Мир информационный безопасности подвергался государственному регулированию с самых первых дней своего существования, хотя поначалу это регулирование не имело ничего общего с вопросами честной конкуренции. Первые действия касались нераспространения: государство использовало экспортные лицензии и контроль над финансированием исследований, чтобы ограничить доступ к криптографии на как можно более долгий срок. Этот процесс прекратился лишь к началу нынешнего века.

Ландфехр (Landwehr) описывает попытки правительства США разобраться с проблемой "лимонного рынка" в мире компьютерной безопасности, начатые в середине 1980-х. Во-первых, речь идет об исправлении схемы государственного тестирования и сертификации ПО (о так называемой "Оранжевой Книге", "Orange Book"), но это исправление лишь породило новые проблемы. Желание менеджеров упростить процесс сертификации самого свежего софта привело к тому, что производителям было

достаточно показать, что процесс начат, хотя зачастую он так никогда и не заканчивался. Также возникали проблемы взаимодействия с системами союзников - Англии, Германии и пр.

Регулирование значительно улучшилось, когда неудачи рыночного механизма в индустрии информационной безопасности стали ясны. Евросоюз принял документ "Network Security Policy", который установил общеевропейский ответ на атаки на информационные системы. Это послужило началом применения экономических мер при планировании государственного управления. Другой пример: комментарии правительства Германии по поводу инициативы Trusted Computing. Они сильно повлияли на Trusted Computing Group, заставив ее согласиться с принципами членства, исключающими дискриминацию небольших предприятий. Недавно Еврокомиссия высказывала свои соображения об экономических последствиях механизмов безопасности Windows Vista.

По статье Росса Андерсона и Тайлера Мура "Information Security Economics - and Beyond"

Трагедия общин и вопрос ответственности

Еще один важный вопрос, поднятый патриархом экономического анализа информационной безопасности Россом Андерсоном (Ross Anderson): кто отвечает за безопасность? Очевидно, что ответственность за безопасность должна возлагаться на того, кто имеет возможность ее обеспечивать. Однако в условиях, когда компьютер домохозяйки может использоваться для атаки на сайт Microsoft, а неграмотно настроенный SMTP-сервер - поставить под удар всю сеть, в которой он находится, это далеко не тривиальная проблема. Сколько вы готовы заплатить за то, чтобы обеспечить безопасность Microsoft? Думаю, немного. И уж конечно, вы практически ничем не рискуете, отказываясь от добровольной помощи редмондскому гиганту - Microsoft вряд ли будет судиться с вами в случае участия вашего компьютера в DDoS-атаке (как мы уже видели, бороться с отдельными участниками распределенной угрозы никто не будет, кроме разве что RIAA и MPAA, но этот клинический случай мы не рассматриваем).

В экономике такая ситуация известна под названием "трагедия ресурсов общего пользования" (Tragedy of the Commons) и описывается обычно так. Пусть 100 жителей деревни пасут

своих овец на общинной земле. Если кто-то из них добавляет лишнюю овцу в свое стадо, он получает существенную выгоду, тогда как остальные 99 жителей страдают лишь от незначительного ухудшения состояния пастбища. Вряд ли они поднимут вой по этому поводу - скорее сами добавят по овце. Со временем такая стратегия приводит к безграничному росту общего числа овец и полному истощению земли.

Подобные ситуации, когда эгоистичные (или рациональные, что в данном случае одно и то же) действия отдельных участников сообщества по отношению к общественному ресурсу приводят к краху всей системы, наблюдаются в компьютерной безопасности буквально на каждом шагу. Общественным ресурсом в данном случае является общая безопасность информационной среды, стоимость которой распределяется между участниками. Например, пользователь локальной сети, купив соответствующее ПО и упрочив защиту своего компьютера, повышает общую безопасность.Однако стимул вкладывать личные деньги, по сути, в общее дело невелик: возникает соблазн подождать, когда это сделают другие (а они этого не сделают по тем же самым причинам). Аналогичным образом замена устаревших технологий новыми безопасными аналогами (например, DNSSEC вместо существующего DNS) идет черепашьими темпами: поскольку на начальном этапе (когда пользователей новой технологии немного) затраты велики, каждый участник рынка ждет, когда их возьмет на себя кто-то другой. Социальных механизмов борьбы с этим явлением пока не существует.

Андерсон приводит еще один пример, связанный с ответственностью: он касается банков и их взаимоотношения с клиентами. Если кто-то украл деньги с какого-то банковского счета, то виноватым может оказаться как банк (например, использовалась небезопасная инфраструктура для аутентификации пользователей или украдена база данных), так и клиент (например, записал пароль на бумажке, наклеенной на монитор офисного компьютера, а файл с цифровым сертификатом положил на "Рабочий стол"). По законодательству США, действует презумпция виновности банка: ему придется доказывать, что "лоханулся" пользователь, либо возмещать убытки. Во многих европейских странах ситуация противоположная. Нетрудно догадаться, что банки США в среднем лучше и эффективнее защищают свои системы, хотя и тратят на это меньше денег.

Нельзя продать? Отдадим даром!

В условиях отсутствия легального рынка уязвимостей, единственное, что получает исследователь, публикующий свои изыскания - известность, имя и славу. В такой ситуации говорят об "экономике репутаций". Когда-то именно вопрос репутации был основным движущим фактором развития вредоносного кода. Впрочем, в индустрии безопасности имя можно конвертировать в деньги сравнительно просто: громкое "разоблачение" может стать неплохим пиаром и привести к исследователю толпы клиентов, жаждущих безопасности (даже от мнимых угроз).

Во время обсуждения ситуации вокруг руткита Blue Pill Виталий Камлюк сказал, что, с его точки зрения, публикация кода руткита была поступком не очень этичным и может оказаться помощью "темной стороне". Мы попросили Джоанну Рутковску прокомментировать это мнение.

"Конечно, у меня другой взгляд. Во-первых, заметьте, что эксплойты и proof-of-concept-код (например, Blue Pill) не создают новых уязвимостей в системе - они только используют уже существующие уязвимости. Если бы компьютерные системы были правильно спроектированы и реализованы, эксплойтов не было бы. Публично доступные эксплойты и другой подобный код только показывают возможные опасности и позволяют изучать возможные способы противодействия таким проблемам.

Должна сказать, что очень удивлена позицией, высказанной "Лабораторией Касперского". Как производитель систем безопасности, они должны быть благодарны другим исследователям за публикацию своих результатов, которые позволяют (например, самой "Лаборатории Касперского") работать над предотвращением таких угроз.

Пожалуйста, учитывайте также, что опубликованная версия Blue Pill не может считаться malware, поскольку не содержит никакого вредоносного кода. Эта базовая версия лишь устанавливает очень "тощий" гипервизор и перемещает запущенную в данный момент ОС в виртуальную машину, контролируемую гипервизором. Ничего больше! Конечно, кто-то может использовать этот скелет для создания перехватчика паролей, но точно так же можно представить себе создание системы-ловушки (honeypot system), отладчика или даже anti-rootkit-системы на основе нашего скелета.

Более того, Blue Pill не использует никаких дыр, а полагается только на документированную функциональность, как она описана в руководствах AMD. Так что его даже нельзя классифицировать как эксплойт."

Почем лимоны?

Впрочем, описанные проблемы - это не все плохое, что бывает на свете. Даже если мы распределим ответственность правильно, это будет только шагом на пути к безопасности. Дело в том, что в современных условиях рыночные механизмы не могут обеспечивать выигрыш более защищенных систем в свободной конкурентной борьбе. Это связано с тем, что рынок ИТ представляет собой рынок с асимметричной информацией, на котором продавец обладает более подробными и точными данными о товаре, чем покупатель.

За изучение подобных рынков американский экономист Джордж Акелроф получил в 2001 году Нобелевскую премию по экономике. Предложенная им модель довольно проста; она носит название "лимонного рынка". Рассмотрим рынок подержанных машин. Допустим, что на нем продаются как хорошие авто ("сливы", объективная цена которых - $3000), так и "битые" ("лимоны", стоящие реально $1000), причем покупатель не может отличить одни от других (пока не проедет пару тысяч миль). Если предположить, что вероятность "наколоться" составляет 50%, складывается впечатление, что равновесная рыночная цена должна быть по $2000 за машину; однако по такой цене никто не будет продавать "сливы", и рынок заполонят "лимоны". Как только покупатели это обнаружат, рыночная цена упадет вообще до $1000.

Мораль: в условиях отсутствия информации у покупателей рынок подталкивает производителей к поставке некачественного товара. Именно это и происходит с безопасностью: несмотря на все исследования, пользователь никогда не может достоверно оценить степень защищенности того или иного продукта, и ему приходится полагаться на заявления производителя. К чему это приводит, мы уже видим.

Блошиные рынки

Можно пытаться решить проблему оценки надежности экономическими методами. Безопасность системы может быть оценена через стоимость новой (zero-day) уязвимости, найденной для этой системы. Это логично: чем надежнее система, тем

больше людей ей доверяют, тем эффективнее будет zero-day-атака и тем дороже информация для ее осуществления; и наоборот: если система надежна, нам придется крепко поработать и потратить много денег, чтобы ее взломать. Проблема в том, что открытого легального рынка уязвимостей, который бы позволял оценивать их настоящую стоимость, в настоящий момент практически не существует, и даже не вполне понятно, каким он должен быть, чтобы приносить наибольшую пользу обществу.

Райнер Бёме (Rainer Bцhme) рассматривает несколько типов рынков уязвимостей. "Баг-челленджи" (bug challenges) и "баг-аукционы" (bug auctions) относятся к самым простым и известным видам. Например, Дональд Кнут обещает выплачивать за каждую найденную ошибку в издательской системе TeX некоторую сумму, увеличивающуюся со временем. Аналогично Mozilla Foundation платит исследователям за уязвимости, найденные в браузере Firefox. В зависимости от заявленной цены исследователь может предпочесть продать уязвимость вендорам, вместо того чтобы использовать ее для создания эксплойта. Для этого, однако, цена должна быть достаточно большой и увеличиваться с ростом количества установок и внедрений.

"Несмотря на возможность денежного выражения стоимости эксплойта, я бы не назвал этот подход прекрасным рынком уязвимостей, поскольку соответствующий рыночный механизм обладает множеством проблем, - пишет Бёме. - Цена на этом рынке определяется покупателем (то есть вендором ПО. - И.Щ.), а не является результатом договоренности". В результате она представляет собой только нижнюю оценку, и использовать ее затруднительно.

Еще один вариант: "брокеры уязвимостей" - здесь речь идет о компаниях, скупающих информацию о дырах в безопасности для ее перепродажи "хорошим людям" (вендорам ПО, корпоративным пользователям и т. д.). Такие компании существуют - например, iDefense, TippingPoint, Digital Armaments и др. С точки зрения общественной пользы, этот подход тоже далек от идеала - потому, в частности, что не сообщает никакой информации (о ценах уязвимостей и надежности продуктов) широкой публике. К тому же он вызывает соблазн у "плохих людей" (преступности) получить доступ к упомянутой информации.

Еще один вариант рынка - "exploit derivatives" (мне не удалось подобрать хорошего перевода этого термина). Суть его в том, что торговля на рынке происходит не самими эксплойтами и информацией об уязвимостях, а обязательствами выплатить определенную фиксированную сумму при наступлении того или иного события - например, обнаружения (или необнаружения)

уязвимости какого-то конкретного продукта в конкретный момент времени. В этом случае стоимость подобных обязательств будет указывать на предполагаемую надежность продукта.

Так, производитель ПО, уверенный в своем продукте, может активно покупать контракты, по которым производятся выплаты, если уязвимость не будет обнаружена, - тем самым поднимая стоимость контракта практически до номинала. Аналогичным образом исследователь, обнаруживший уязвимость в продукте, считавшимся безопасным, может скупить контракты, выплаты по которым производятся в случае обнаружения уязвимости, а потом раскрыть свою информацию и продать контракты по более выгодной цене.

Наконец, Бёме рассматривает страхование - которое, обладая многими достоинствами, слабо распространено по разным техническим причинам.

Однако, несмотря на неплохую теоретическую проработку этого вопроса, легально продать найденный эксплойт сейчас непросто. Чарли Миллер пишет о своем опыте участия в легальном рынке уязвимостей и перечисляет связанные с ним проблемы: быстрое и неожиданное устаревание и обесценивание информации, отсутствие прозрачности в ценах, сложность поиска и проверки надежности покупателя, трудность доказательства обладания эксплойтом без раскрытия важной информации о нем.

Из двух попыток продажи уязвимостей Миллеру удалась лишь одна - да и та благодаря личным связям. Таким образом, можно заключить, что эффективного легального рынка в данный момент не существует.

Если ты такой распространенный, почему ты такой дырявый?

Кроме упомянутых в статье, есть и другие причины, вследствие которых производителю софта (и информационных систем вообще) невыгодно заниматься его безопасностью. Андерсон выделяет, например, стремление как можно быстрее захватить рынок и "замкнуть" на себе пользователей с помощью проприетарных технологий. Здесь работает так называемый закон Меткалфа (полезность продукта пропорциональна числу его пользователей), хорошо проявивший себя в ситуации с пакетом MS Office: даже сейчас, несмотря на усилия по распространению открытых стандартов для офиса, старые бинарные форматы файлов (doc, xls) остаются стандартом де-факто в документообороте и замыкают пользователей на продукты

Microsoft. В этой ситуации разработчики платформы (например, Windows) должны на этапе захвата рынка как можно больше упростить жизнь разработчикам стороннего софта - а значит, не могут обременять их заботой о безопасности. "Мы доставим товар в этот вторник, но сделаем все как надо только к третьей версии - идеально рациональное поведение в условиях многих рынков", - пишет Андерсон - и именно это мы наблюдаем в попытках радикально улучшить безопасность Windows Vista.

Заключение

Исследование вопросов информационной безопасности давно вышло за рамки интересов технических специалистов и довольно активно исследуется представителями гуманитарных дисциплин - в первую очередь экономистами. Возможно, ключ к нашей безопасности лежит именно в этих исследованиях, а не в еще более быстром обновлении антивирусных баз и даже не в хитрых технологиях, против которых обязательно найдутся соответствующие технологии у другой, враждебной стороны.

Литература

[1] Don Jackson/SecureWorks, "Gozi Trojan" (технический отчет).

[2] Scott Berinato/CIO, "Who's Stealing Your Passwords? Global Hackers Create a New Online Crime Economy".

[3] Ross Anderson, "Why Information Security is Hard - An Economic Perspective".

[4] Ross Anderson, Tyler Moore, "Information Securty Economics - and Beyond". Там же.

[5] Rainer Вцhme, "Vulnerability Markets: What is the economic value of a zero-day exploit?".

[6] Charlie Miller, "The Legitimate Vulnerability Market: Inside the Secretive World of 0-day Exploit Sales".

книги: Недетские игры

Автор: Киви Берд

Вряд ли хоть кто-то, пребывая в здравом рассудке, станет отрицать, что учиться на своих ошибках - это признак ума. Признак же мудрости - способность учиться на ошибках других. Однако Эд Фелтен, профессор Принстона и видный специалист по защите информации, недавно отметил, что специалисты по компьютерной безопасности, увы, регулярно демонстрируют неспособность учиться на ошибках - как чужих, так и собственных. То ли старательно скрывают уже допущенные промахи, то ли притворяются, будто их просто не существует.

8/12

В самую популярную в мире многопользовательскую онлайновую игру World of Warcraft, по состоянию на лето 2007 года, играли 8 млн. человек, каждый из которых платит за право участия в ней 14 долларов в месяц. По оценкам аналитиков, к 2009 году игровой рынок достигнет 12 млрд. долларов.

Сформулированная Фелтеном идея, конечно же, не была внезапным откровением. О неблагоприятном положении дел с компьютерной безопасностью прекрасно осведомлены все эксперты и даже многие несведущие в этой области люди. Постоянно прилагаются усилия, чтобы переломить унылую тенденцию и перестать, наконец, наступать на одни и те же грабли. Частью этой работы стала новая книга американских авторов Грега Хоглунда и Гэри Макгроу "Эксплуатация онлайновых игр: жульничество в массивно-распределенных системах"["Exploiting Online Ga-mes: Cheating Massively Distributed Systems" by Greg Hoglund and Gary McGraw, Addison-Wesley Professional, 2007, www.exploitingonline-games.com.]. В книге подробно рассказывается о промахах, допускаемых игровыми компаниями, и о последствиях этих промахов. Фирмам, разрабатывающим компьютерные игры, это издание поможет извлечь уроки из своих ошибок, да и из ошибок коллег по индустрии. По этой книге можно научиться заранее замечать ловушки, подстерегающие разработчика, - и избегать их.

Волею судьбы выход книги совпал по времени с большущим интернет-скандалом вокруг популярного онлайнового казино AbsolutePoker.com (См. заметку "Абсолютная афера" в КТ #708 -

Прим. ред.). Завсегдатаи этого сайта - заядлые картежники - вдруг стали замечать, что некоторые игроки демонстрируют поистине сверхъестественные способности. Своими точными ходами, умелыми ставками и регулярными крупными выигрышами эти счастливчики попирали все законы теории вероятностей, словно видя карты соперников насквозь. Администрация сайта-казино, следуя традиции, ни в какую не признавала очевидные факты жульничества и категорически не желала проводить расследование. Тогда за дело взялись сами посетители сайта. Они собрали массу информации, документально подтверждающей мошенничество, которое стало возможным вследствие слабостей программного обеспечения. Улики, изобличившие одного из технических сотрудников казино, оказались столь вескими, что компания была вынуждена официально извиниться и привлечь к судебной ответственности собственные кадры.

Зачем пишутся такие книги?

В двух словах, книга Хоглунда и Макгроу о том, как жульничают в играх. Понятно, что всякая игровая компания к подобному жульничеству в своем хозяйстве и к его пропаганде относится в высшей степени нетерпимо. Если хитрости и манипуляции становятся крупномасштабными, то игрокам, которые в подобных вещах не участвуют, это рано или поздно надоест и они уйдут искать развлечений в более приличном месте. Поэтому разработчики игр предприняли ряд шагов, направленных на укрепление защиты программ против мошенничества и злоупотреблений. Одни контрмеры, вроде негласной слежки за каждым из игроков и содержимым их компьютеров с помощью шпионов-руткитов, заведомо спорные. Другие контрмеры имеют правовые перекосы, закладываемые в

чрезвычайно жесткие лицензионные соглашения и условия пользования игрой. Третьи, наконец, носят характер чисто технической защиты, вроде шифрования коммуникаций между клиентом и сервером. Правда, как показывает анализ, криптографию в играх обычно реализуют весьма неумело. А потому, надеются авторы книги, сделанный ими тщательный разбор известных типов хакерских атак должен существенно помочь разработчикам игр в укреплении безопасности их программ.

Кроме того, Хоглунд и Макгроу выдвигают еще несколько веских, по их мнению, доводов относительно полезности своей работы. Во-первых (этот аспект многократно подчеркивается и другими авторами по самым разным поводам), в виртуальных мирах игр ныне крутятся реальные и весьма большие деньги. Во-вторых, огромное множество игроков по сию пору совершенно не в курсе, каковы подлинные масштабы жульничества. И в-третьих, безопасность программ для онлайновых игр имеет не просто много, а очень много критически важных моментов, которые напрямую связаны с проблемами безопасности других, более важных разновидностей программного обеспечения.

Как практикующие эксперты по компьютерной безопасности, авторы книги уверены, что для всестороннего понимания системы надо знать не только как она работает, но и как она ломается. Единственный же путь к этому - выявлять и досконально изучать все слабые места системы.

Почему игры, или о чем эта книга

Завтра

Массивно-распределенные онлайновые игры имеют чрезвычайно сложное программное обеспечение. Благодаря гигантскому числу пользователей это ПО постоянно проверяет на прочность распределенные клиент-серверные архитектуры. Поскольку почти любое современное ПО в конечном счете становится массивно-распределенным, сегодняшние игры – это завтрашний день остальных программ.

Предисловие, вступление и первая глава "Эксплуатации онлайновых игр" дают развернутое объяснение причин,

побудивших авторов взяться за описание средств и методов жульничества. Хоглунд и Макгроу принадлежат к довольно узкой группе специалистов, умеющих работать в стиле "хакинг для защиты". Подробно исследуя всевозможные уязвимости систем, они выпустили уже несколько книг об эксплуатации слабостей защиты программного обеспечения. По всеобщему признанию это весьма полезные руководства для тех, кто пытается строить надежные, хорошо защищенные программы.

Итак, почему же на сей раз особое внимание авторы уделили играм? Прежде всего потому, что уже сформировалась крупная виртуальная экономика, которая на множестве направлений пересекается с "реальной" экономикой и оперирует вполне реальными деньгами. С тех пор, как геймеры начали продавать ценимые в играх способности, "игровое золото" и даже целиком персонажей, объекты игр обрели конкретную денежную стоимость в реальном мире. Одновременно мир игр, вроде World of Warcraft, EverQuest и онлайнового покера, привлек интерес и криминального мира. Торговля игровыми объектами ныне тесно переплетена с онлайновым мошенничеством, хищениями персональных данных и отмыванием денег. Так, в разгар финальных игр Суперкубка по американскому футболу сайты главных стадионов США были заражены троянцем, который наряду с кражей финансовой и персональной информации пользователей целенаправленно искал и похищал из компьютеров данные аккаунтов участника World of Warcraft.

Вторая глава ("Хакинг") содержит развернутое обсуждение разнообразных способов манипуляции играми. Большинство этих способов изложено на концептуальном уровне, хотя некоторые вещи разбираются очень подробно и с примерами, включая макрокоды и подпрограммки на языке C. Здесь же анализируются контрмеры, применяемые в играх для борьбы с жульничеством, и несколько популярных способов для обхода этих контрмер.

Глава три ("Деньги") на конкретных примерах исследует работу виртуальной экономики игровых миров. И хотя в предисловии подчеркивается важность экономического аспекта, в самой книге об этом говорится скупо. Впрочем, необъятное, как известно, объять нельзя.

Не может похвастать широтой охвата и глубиной и четвертая глава ("Адвокаты"), в которой собраны сведения об американских законах, регулирующих копирайт и смежные области защиты интеллектуальной собственности, а также рассмотрены всевозможные юридические и технические зацепки, встраиваемые разработчиками ПО в EULA (End User License Agreement, лицензионное соглашение конечного пользователя).

Пятая глава посвящена ошибкам в программном обеспечении игр. Точнее, тому, каким образом геймеры могут использовать баги в собственных целях - для взаимодействия со сложными функциями и состояниями игры.

В главе шестой разбираются инструменты и техники, применяемые для манипуляций клиентским программным обеспечением. С определенными оговорками можно утверждать, что содержание главы - это та самая суть, ради которой и была написана книга. Ибо именно с толстого (то есть функционально продвинутого) клиента идет подавляющее большинство злоупотреблений и манипуляций слабостями игровой системы. Глава в изобилии насыщена примерами и кодами на языке Си; в данном контексте это вполне оправданно.

Седьмая глава ("Строительство ботов") тематически тесно связана с предыдущей и столь же насыщена строками С-кодов, используемых при создании программных роботов, жульничающих в играх ради преимуществ для своих владельцев.

Глава восьмая - это, можно сказать, другое ответвление главы шесть, направленное в сторону обратной инженерной разработки ПО. Здесь тоже рассмотрен разнообразный инструментарий, применяемый для вскрытия программ. Дается и весьма подробный обзор базовых функций ассемблера.

Девятая глава посвящена продвинутому хакингу игр. В ней главным образом разбирается модифицирование программ, управляющих работой клиента или альтернативного игрового сервера.

Финальная, десятая глава ("Безопасность программ превыше всего") предназначена, судя по всему, для красивого перехода от технических подробностей к выводам самого общего характера. Глава начинается несколько запоздалым заявлением о том, что главная цель книги - "понять важность безопасности в массивно-распределенных программных системах, имеющих миллионы пользователей". Эта цель, напомним, прописана в подзаголовке книги, однако за подробным разбором приемов хакинга углядеть ее не так-то просто. Чтобы компенсировать это упущение, глава 10, по сути дела, представляет собой краткий обзор множества полезных, но, строго говоря, общеизвестных основ в деле защиты программного обеспечения.

Учиться на ошибках

Еще

Для Хоглунда и Макгроу, авторов новой книги о хакинге онлайновых игр, это далеко не первая работа по компьютерной безопасности. Они уже выпустили с полдюжины книг, посвященных руткитам, безопасному программированию и взлому кодов. Подробности можно найти на сайтах www.buildingsecurityin.com и www.rootkit.com.

При рецензировании любой книги считается дурным тоном затевать разговор о том, чего в тексте нет. Ибо рецензия по определению должна быть посвящена тому, что в книге есть. Однако для данной статьи новое исследование о хакинге игр - это не столько тема рецензии, сколько наглядный повод обсудить общую ситуацию в мире компьютерной безопасности. А потому вполне уместно перечислить и те моменты, которые в книгу не вошли или обсуждаются лишь мимоходом.

Например, все технические главы работы посвящены тому, как серверы системы компрометируются со стороны клиентского ПО. Но нет почти ничего о том, как общие слабости игровой системы могут делать крайне уязвимыми для сетевых атак клиентскую сторону и компьютеры пользователей. Дыры в клиентском ПО могут открывать компьютер для проникновения шпионов, похищающих чувствительную информацию о пользователях либо прокладывающих путь другим вредоносным программам. В реальном мире есть множество такого рода проблем, тесно связанных с другими клиентскими программами, вроде средств для быстрых коммуникаций или пиринговых файлообменов.

Кроме того, за рамками книги осталось множество проблем, связанных именно с безопасностью массивно-распределенных систем, насчитывающих сотни тысяч одновременно играющих пользователей. Например, совсем не затронут социальный инжиниринг применительно к совместной работе больших групп людей. То же касается самозарождающихся (emergent, эмерджентных) новых свойств системы в целом, возникающих при взаимодействии простых функций, оперирующих на очень большом числе узлов. Не анализируется мощь согласованных действий пользователей в крупных распределенных системах. Наконец, нет ни слова о взаимосвязи между игровыми сетями и ботнетами, сетями вредоносных программных роботов, в последнее время ставшими головной болью для компьютерной безопасности.

Если же копнуть глубже, неизбежно возникнет вопрос о необходимости открытого обсуждения всех уязвимостей. Книга Хоглунда и Макгроу в этом отношении может служить образцом. В индустрии компьютерных игр, спору нет, ставки не столь высоки, как в авиации [см. врезку], однако возникающие и тут и там проблемы имеют много общего. Как и в авиации, разработчики делают серьезные финансовые вложения в успех и производительность своих систем. Однако и остальные участники ставят на кон достаточно много. Онлайновый виртуальный мир, подобный World of Warcraft, порождает собственную экономику, и постоянно расширяется круг людей, чье благосостояние полностью или частично зависит от заработков внутри игровых миров. Валюта игровых миров обменивается на доллары и евро. Экономисты по сию пору оживленно спорят о точном смысле и стоимости валового продукта в виртуальных пространствах, однако в смысле делания денег виртуальная экономика столь же реальна, как и купля-продажа акций на бирже.

Открытая модель против закрытой

Оживленные, порою даже очень острые дискуссии о целесообразности полного раскрытия уязвимостей идут в компьютерном мире много лет. За это время сторонники секретности выдвинули горы самых разных аргументов этического, правового и технического характера. Тем не менее подавляющее большинство независимых экспертов по безопасности продолжают стоять на своем: и специалисты, и общество только выигрывают, если четко представляют, как работают технологии, от которых все зависят.

В современном мире уже стало нормой положение, при котором человек вынужден ставить свои деньги, время, приватную информацию, а порой и собственную жизнь в прямую

зависимость от того, надежно ли сработают те или иные технологии. Технологии эти могут сильно отличаться друг от друга, сделать между ними правильный выбор не так-то просто, и люди, естественно, нуждаются в помощи специалистов. В качестве самой яркой иллюстрации этой идеи обычно приводят безопасность авиаперелетов. Здесь ставки максимально высоки, и у пассажиров должна быть полная уверенность, что все потенциальные проблемы будут выявлены и исправлены. Никто не стал бы мириться с ситуацией, когда изготовитель самолетов скрывает причину катастрофы или препятствует расследованию. Аналогично, люди не будут иметь дел с компанией, которая лжет публике о безопасности полетов и отрицает наличие проблем, хотя ей известно обратное. Именно огласка обнаруженных слабостей, тщательное расследование аварий и умение учиться на ошибках сделали воздушные перелеты действительно безопасными.

Если авиация демонстрирует преимущества открытости, то электронное голосование, напротив, выпукло иллюстрирует все те беды, что вызваны чрезмерной секретностью. Пользователям систем электронного голосования - то есть всем гражданам - не дозволено знать, как работают эти машины. Обычно людям сообщают лишь то, что все машины голосования прошли сертификацию, однако суть этого важного процесса окружена зачастую непроницаемой завесой тайны. По мнению властей, подробности этой технологии граждан не касаются. Последствия же такого подхода хорошо известны. При независимой проверке выясняется, что конструкция систем голосования очень слаба, дыры в безопасности годами остаются незалатанными, а общий прогресс идет чрезвычайно медленно. И даже в ситуациях, когда техника в ходе реальных выборов явно срабатывает не так, как должна, бывает очень трудно добиться строгого и объективного разбирательства. Понятно, что доверять таким системам по меньшей мере неосмотрительно.

Масса людей, никоим образом не вовлеченных в онлайновые игры, могут серьезно зависеть от этих виртуальных миров. Таков, к примеру, инвестор, вкладывающий свои пенсионные отчисления в игровую компанию. Или программист, оставляющий приличное место в софтверной компании ради работы над новой игрой. Или, наконец, семья, владеющая ресторанчиком, расположенным напротив штаб-квартиры игровой компании. Для всего этого народа тоже крайне важно, чтобы технология, на которую они поставили, была серьезной и надежной. Ну а уж те

люди, что относятся к гигантскому сообществу геймеров, перед тем как отдавать свои кровные деньги за игровую программу или онлайновую подписку, наверняка хотели бы быть в курсе, насколько хорошо эта программа способна противостоять атакам жуликов и злоумышленников.

Упомянутый в самом начале принстонский профессор Эд Фелтен, оценивая насыщенную примерами хакинга книгу Хоглунда и Макгроу, заметил, что некоторые разработчики игр, возможно, встретят эту работу без энтузиазма, а то и с раздражением. Не исключено, что они даже попытаются обвинить авторов в подрыве безопасности их игрового программного обеспечения. Но это, подчеркивает Фелтен, будет лишь попыткой самообмана. Если кто-то собирается улучшить практикуемые технологии защиты, то честное обсуждение известных проблем, такое, как в книге, - это единственный путь вперед.

Ибо абсолютно всем свойственно делать ошибки. А потому, если в следующий раз захочется сделать лучше, следует учесть не только свои, но и чужие ошибки.

анализы: Машины для голосования в России

Автор: Суслов,Алексей

"Компьютерра" уже не раз писала об электронных устройствах для голосования, особенно использующихся в США. Здесь мы расскажем об опыте применения машин для голосования в России, ведь выборы не за горами, и в декабре многим читателям придется иметь дело с подобными устройствами.

Самая трудоемкая задача для организаторов любых выборов - это подсчет голосов. При традиционной процедуре голосования бумажные бюллетени подсчитываются членами избирательной комиссии вручную. Если избирателей много, эта работа отнимает кучу времени, а результат, вследствие "человеческого фактора", может быть не совсем точным.

Попытки автоматизировать процесс подсчета голосов предпринимаются давно. Первые механические машины для голосования применялись еще на выборах в Рочестере (США) в 1892 году. В начале XX века считалось, что машины надежнее традиционной системы с бумажными бюллетенями, поскольку делают невозможной фальсификацию результата.

Классификация

Исторически машины для голосования эволюционировали следующим образом:

- машины с непосредственным механическим вводом и счетчиком (наподобие одометра в автомобиле);
- машины с использованием перфокарт;
- оптические считыватели бюллетеней;
- электронные машины.

По способам взаимодействия с избирателем эти устройства делятся на две категории:

- непосредственно взаимодействующие с избирателем;
- обрабатывающие бумажный бюллетень для голосования.

С точки зрения безопасности и проверяемости результатов голосования машины принято делить на программно-зависимые (Software Dependent, SD) и программно-независимые (Software Independent, SI). SI-машины предусматривают проверку голосующим правильности учета поданного им голоса и

обеспечивают - даже в случае сбоя, ошибки в программе или механизме машины - возможность корректного подсчета голосов и открытой и ясной процедуры пересчета. В SD-машинах корректность подсчета голосов основывается только на декларациях разработчиков машин.

КОИБы

Системы автоматизации подсчета голосов применяются на выборах в России с 1996 года. Первоначально это были просто сканеры бюллетеней, способные работать только с листами формата А4. Был объявлен конкурс на разработку новых, более совершенных устройств, и с 2004 года на выборах стали применяться комплексы обработки избирательных бюллетеней - КОИБы.

Комплекс представляет собой оптический сканер бюллетеней, расположенный над урной для голосования ("накопителем бюллетеней") и интегрированный с компьютером. Несколько комплексов в пределах одного участка объединены в локальную сеть. К одному из комплексов, который обозначается как "главный", подсоединяются периферийные устройства: принтер, модем. Для уменьшения вероятности выхода из строя всей системы предусмотрена возможность переназначения главного комплекса при сбоях. Комплексы управляются с клавиатуры. Данные о бюллетенях для голосования вводятся с дискет. Сведения о результатах голосования могут быть переданы в территориальную комиссию посредством модема или же на дискете. Идентификация бюллетеней производится по оттиску печати участковой избирательной комиссии, распознаваемой

сканером.

Избиратели обычным образом заполняют бюллетени, которые затем считываются сканером и попадают в урну для голосования.

СМИ дают неоднозначные оценки опыта применения КОИБ на прошедших выборах. Так, по официальным данным, использование комплексов позволило уменьшить количество ошибок при подсчете голосов. Контрольные же ручные пересчеты голосов на нескольких участках не выявили сколь-нибудь существенных различий в цифрах. Главными причинами ошибок распознавания называются плохое качество бумаги, типографский брак при печати бюллетеней, слабые оттиски печати участковой комиссии.

Однако неофициальные данные свидетельствуют о наличии более серьезных проблем. Вызывает опасения использование в системе модема, что дает теоретическую возможность незаметного дистанционного управления устройством. Другая претензия наблюдателей - отсутствие обязательного ручного пересчета бюллетеней. Решение о пересчете принимает сама комиссия, наблюдатели потребовать пересчета не могут. В связи с этим появляются сомнения в правильности подсчета голосов, как было, например, на местных выборах в Архангельской области в 2004 году и на выборах в Московскую городскую думу в 2005 году.

Электронные комплексы (КЭГ)

Ждем

Когда эта статья готовилась к печати, в редакцию был прислан другой материал на ту же тему, причем за подписью топ-менеджеров (если только этот термин применим в данном случае) Центризбиркома. Самое приятное, что на статью их вдохновила одна из недавних публикаций "КТ". В ответ мы – не терять же такую возможность! – запросили некоторые дополнительные подробности и теперь ждем ответа. Ну а к концу ноября мы готовим тему номера, посвященную всем сторонам избирательного процесса, а также обзор передовых разработок в области электронного голосования. – Л.Л.-М.

Более прогрессивные устройства - комплексы электронного голосования (КЭГ) - представляют собой систему с сенсорным

экраном, на котором избиратель отмечает выбранные партии и кандидатов. Бумажный бюллетень для голосования при этом не используется; точнее, голосовать по старинке можно "в случае, если избиратель, предварительно познакомившись с правилами голосования на КЭГ на тренажере, отказывается от электронного голосования…".

Комплексы для голосования соединяются в сеть с центральным узлом в виде так называемого сетевого контроллера. Его основная функция - сбор итоговых сведений о результатах голосования, индикация хода голосования (подсчет проголосовавших по участку), распечатка результатов.

За день до голосования производится тестирование комплексов, заключающееся, по сути, в проверке правильности суммирования голосов за выбираемые последовательно партии или кандидатов. За каждую позицию бюллетеня при тестировании отдается один голос. Конечно, эта процедура служит скорее для успокоения наблюдателей и членов комиссии, поскольку выявить неочевидные проблемы (ошибки) в работе комплексов не может.

Для исключения возможности повторного голосования используются карточки со штрих-кодом. Избиратель выбирает карточку из стопки, член комиссии "активирует" ее - с помощью сканера штрих-кода считывает номер карточки, который запоминается в центральном блоке системы. Избиратель подносит карточку к считывателю устройства для голосования, после чего ее номер запоминается в списке уже проголосовавших карточек. Далее производится выбор партий/кандидатов на сенсорном экране, а затем на специальном принтере распечатывается мини-протокол с выбранными позициями, который через небольшое прозрачное окошко на принтере сверяется с сенсорным экраном. При подтверждении голосования лента на принтере проматывается вперед, и результат становится невидимым. Сама по себе карточка со штрих-кодом не несет никакой "секретной" информации и печатается на обычном принтере с помощью несложной программы. По сути, код на карточке является одноразовым паролем доступа к функции голосования, действующим с момента активации карточки до считывания ее комплексом, после чего код помещается в базу уже голосовавших кодов и не может быть использован повторно.

По завершении голосования результаты распечатываются, контрольные ленты из принтеров изымаются и опечатываются с целью возможной проверки результатов. Данные в электронном виде записываются на карты памяти, которые передаются в вышестоящую комиссию.

Комплексы электронного голосования уже использовались на выборах в Великом Новгороде 8 октября 2006 года. Никаких серьезных проблем с ними не было, а два отмеченных недостатка - мелкий шрифт интерфейса и неоднозначность процедуры завершения голосования - разработчики пообещали устранить в следующей версии.

Однако с точки зрения проверяемости выборов электронным комплексам еще далеко до идеала. Так, опыт новгородских выборов показал, что на некоторых участках контрольные принтеры не были подключены. Несмотря на то что в последней версии инструкции ЦИК есть требование об обязательном подключении таких принтеров, пересчет результатов по данным бумажных контрольных лент после голосования не предусмотрен и может быть произведен только по решению суда или вышестоящей комиссии, что, конечно же, снижает степень доверия к результатам выборов.

Что можно посоветовать читателям, которые будут участвовать в выборах с использованием электронных устройств? При голосовании с помощью КОИБ важно не сминать и не складывать бюллетени, а также опускать их в приемник бюллетеней по одному. При использовании КЭГ следует убедиться, что предыдущий избиратель закончил голосовать: горит зеленый индикатор, на контрольном принтере виден чистый кусок бумажной ленты, на экране надпись: "Воспользуйтесь картой доступа". Перед подтверждением результата голосования необходимо проверить, правильно ли напечатаны выбранные позиции на бумажной ленте. Наблюдатели же при использовании КЭГ должны следить за активацией карточек по показаниям индикатора, а по показаниям счетчика - за тем, чтобы избиратель голосовал только по одной - полученной им - карточке. Теоретически возможна ситуация, когда избиратель выносит активированную карточку, не проголосовав по ней, после чего кто-то голосует по нескольким карточкам "правильным образом", благо пронести на участок несколько карточек легче, чем пытаться засунуть в урну для

голосования стопку бюллетеней.

наука: Наноалхимия

Автор: Губайловский Владимир

"Свинец расплавлен… Пора… Рудольф тингирует сам. Проекция исполнена мастерски - металл начинает кипеть… Император погружает оплодотворенную "матрицу" в холодную водяную ванну. Закатав рукав, собственноручно достает из купели плод и поднимает слиток на свет: нежное мерцание чистейшего новорожденного серебра…"

С того времени, которое Густав Майринк описал в романе "Ангел Западного окна", прошло четыре века. Император Рудольф умер в 1612 году в Праге. Он был покровителем Тихо Браге и Иоганна Кеплера. Он был алхимиком.

Алхимия переживала закат цвета киновари и отступала в тень. Ее место занимали естественные науки. Их пробуждение случилось в ту же эпоху. Корреспондентом императорского астролога Иоганна Кеплера был Галилео Галилей. XVII век стал началом экспериментальной науки, то есть науки в ее современном смысле.

Но читая и слушая многочисленные интервью доктора физико-математических наук, член-корреспондента РАН, и. о. вице-президента РАН, директора Института кристаллографии РАН, главного идеолога российского нанопроекта Михаила Ковальчука, я вдруг увидел под флером наукообразных терминов и рассуждений принципы алхимии, которые не были востребованы триста лет.

Приведу несколько высказываний Ковальчука из интервью, которое он дал журналу "Итоги" ["Итоги", номер 24 (574) от 11 июня 2007 года. Фотография Михаила Ковальчука украшает обложку журнала. Интервью озаглавлено не без претензии: "Нано домини", что можно перевести с латыни примерно так: "Это Нано, Господи!"]. (Рассуждения о великой российской науке, молочных реках и кисельных берегах опускаю.)

М.К.: Наука в современном понимании существует несколько сотен лет. Как она развивалась? По мере роста наших представлений о мире и расширения экспериментальных возможностей ученые вычленяли из единой и неделимой природы отдельные сегменты, доступные для изучения. Писали формулы - получили математику. Смотрели в лупу или подзорную трубу - появилась физика. Сливали жидкости - вышла химия <…> Углубившись в детали, пусть даже крайне важные, мы потеряли некую общую цель.

Современная наука началась с эксперимента. Галилей бросал свинцовые шары с Пизанской башни. Это все знают. Но почему он решил, что бросать надо свинцовые шары, а не, скажем, пух и перья, ведь выводы, к которым он пришел, равно верны и для перьев, и для шаров?

Галилей выбрал те объекты, для которых сопротивлением воздуха можно пренебречь. Если бы он этого не сделал, он не увидел бы существа события - оно бы потонуло в помехах. Главное открытие Галилей сделал еще до того, как бросил первый шар. Он понял, что для постановки эксперимента необходимо научиться пренебрегать - то есть абстрагироваться от бесконечного множества условий, несущественных для решения поставленной задачи. Такая идеализация, которая спрямляет углы и огрубляет параметры, такая "плодотворная односторонность", дающая возможность исследовать только одно качество объекта, - и есть рождение экспериментальной, современной науки вообще. Чтобы поставить эксперимент, нужно понять, как добиться таких условий, при которых несущественные (не исследуемые в этом эксперименте) взаимодействия пренебрежимо малы. Это умение абстрагироваться и есть специализация. Объект, взятый как целое, "единую и неделимую природу" исследовала именно алхимия, потому что во всем видела подобия и аналогии.

М.К. Все изменилось с появлением информационных технологий <…> Ведь они пронизывают, накрывают все отрасли без исключения. <…> Такое же надотраслевое значение имеют и нанотехнологии. Мы начинаем складывать из атомов новые материалы с заданными свойствами.

Если и можно сравнить нанотехнологии с вычислительными системами, то никак не с современными компьютерами, а, например, с арифмометрами XIX века. Тогда люди умели кое-что считать не вручную, тогда была задумана, хоть и не построена, аналитическая машина Бэббиджа. Но это были только разрозненные попытки.

Прорыв произошел в 1930-е годы, когда увидели свет работы Алана Тьюринга и Алонзо Черча. В них давалось конструктивное определение понятия "вычисление". Любое вычисление удалось свести к набору элементарных операций. Клод Шеннон заметил, что любую функцию, вычислимую по Тьюрингу, можно реализовать в виде электрических схем. Это двойное открытие и стало основой того прорыва, который случился в XX веке и привел к рождению информационных технологий. Предостерегая

от повального увлечения теорией информации, которое прокатилось чуть ли не по всем областям науки в 1940–50-е годы, Шеннон писал, что природа почти никогда не позволяет открыть две свои тайны одним ключом. С информационными технологиями так и случилось. И это почти чудо.

Информационные технологии всё "пронизывают", потому что всё пронизывают вычисления, и мы четко представляем, как с ними работать. А вот пронизывают ли всё нанотехнологии? "Атомные кирпичики" есть, но управлять ими, руководствуясь столь же ясными принципами, какими являются вычислительные операции, мы не умеем, а научимся ли - неизвестно.

М.К. Одной из целей развития науки и техники индустриального общества, того, в котором мы жили до сих пор, было изучение "устройства" человека и его возможностей. Создавая какие-то технические системы, мы постоянно копировали себя, пытались усовершенствовать то, что дано нам природой. Например, подъемный кран - это фактическая имитация руки. В оптических приборах мы имитируем человеческое зрение, в акустических - слух. Когда началось создание интегральных схем полупроводниковой микроэлектроники, создатели компьютеров принимали за образец человеческий мозг.

Трудно копировать то, чего ты не понимаешь и даже не видишь. Точнее, это возможно только в одном случае: если ты изначально уверен в том, что все подобно всему. Макрокосм - микрокосму, природа - человеку, человек - Богу. Это всеобщее подобие и есть главный принцип алхимии.

И подъемный кран, и компьютер, и оптические и акустические приборы создавались вовсе не для того, чтобы копировать человека. При создании каждого прибора или механизма решалась совершенно определенная задача - нужно было реализовать определенную функцию, с которой люди справляются неудовлетворительно (как правило, одну и очень простую): поднять тяжесть, рассмотреть удаленный предмет, сохранить звук. Такие четко отграниченные (специализированные) задачи решать удавалось, но и Галилей, увидевший спутники Юпитера в телескоп, и Эдисон, создавший первый фонограф, и фон Нейман, предложивший архитектуру компьютера, были слишком плохо осведомлены, как соответствующие функции реализуются организмом человека.

М.К. Мы начинаем жить в постиндустриальном обществе, в котором иная цель развития науки и технологий. Это означает

переход от технического копирования "устройства человека" на основе относительно простых неорганических материалов к воспроизведению систем живой природы на основе нанобиотехнологий и самоорганизации.

По простоте душевной я полагал, что "постиндустриальное общество" - это общество, которое переходит от производства материальных объектов - товаров, механизмов - к производству информации. Так считал и Даниэль Белл, сделавший популярным этот термин. По Беллу, главным источником богатства и власти в постиндустриальном обществе выступают не машинные, а интеллектуальные технологии. Знания и права на них, выраженные в патентах и торговых марках, оказываются куда дороже технологических линий. А если верить Ковальчуку, в постиндустриальном обществе почти ничего не изменилось - мы продолжаем копировать человека и природу, правда, при помощи других материалов - не из кремния и железа, а из белков. Но в целом мы продолжаем алхимическое познание.

М.К. Мы изучаем человека и пытаемся скопировать некоторые его свойства <…>. Но это всего лишь способ адаптировать нашу цивилизацию к живому миру, как он был задуман изначально.

Все алхимически точно. Нужно сделать цивилизацию подобной миру, "как он был задуман изначально". Задуман кем? В отличие от Михаила Ковальчука, у меня нет доверительных отношений с Господом Богом, мне Он не сообщал, как все это было задумано.

Современная цивилизация - цивилизация аналитическая. Мы разнимаем мир на части, чтобы понять действующие в нем принципы, а потом пытаемся собрать в целое заново. Так мы познаем мир - познаем конструктивно. Но это трудный путь, потому что необходимо предъявить конструкцию и метод ее построения, которым могут воспользоваться другие.

Я очень не люблю слово "междисциплинарный", которое так нравится Ковальчуку. Дисциплина она дисциплина и есть, тем более если она научная. Между дисциплинами существует только хаос, хаос непознанного. Конечно, может развиться новая наука, которая на более глубоких и общих принципах объединит две научные области, казавшиеся далекими. Но для этого нужно что-то большее, чем называние набора разнородных явлений словом "нано". Это похоже на "междисциплинарную науку", которая исследует яблоки и теннисные мячи, потому что они примерно одного размера.

Чем замечательна алхимия? Ясностью задачи, которая проста, как теорема Ферма. Счастье и бессмертие всем, и пусть никто не уйдет обиженным. Неужели вам жалко двести миллиардов рублей для счастья сограждан? Не жалко. Но у простых и ясных задач бывают невероятно трудные решения (а часто решений просто нет). У алхимиков была надежда - надежда на Бога. Наверное, современные ученые тоже прониклись этой надеждой. Вот только Бог не открывает свои тайны по команде.

Императоры мало изменились за последние четыреста лет. Их сегодняшняя щедрость завтра может аукнуться очень больно.

"Келли позвякивает серебряной цепью, пожалованной ему императором. Накидывая ее на преданно склоненную шею, Рудольф многозначительно произнес: "Серебро к серебру, золото к золоту, господин магистр балаганных наук. Не знаю, откуда у вас пудра, в следующий раз посмотрим, сумеете ли вы ее приготовить. И помни: корона для адептов, а цепи… всегда только цепи!" С таким напутствием, в котором угроза прозвучала весьма недвусмысленно, мы и были отпущены из Бельведера; на сей раз нам не пришлось сводить знакомство с лязгающими железом заплечных дел мастерами".

Героям Майринка удалось получить серебро из свинца. Что-то будет с сегодняшними наноалхимиками? Железо по-прежнему железо.

голубятня: Мы встретились в аду

Автор: Сергей Голубицкий

Наверное, кому-то надеялось, что тема ноутбука Sony Vaio VGN-SZ650N/C тихо свернется в тряпочку и безропотно канет в никуда? Святой наивняк! Дело даже не во мне, а в Sony. Не такая это компания, чтобы просто так вот взять и свернуться: Like No Other! (Как никто другой!) - ее рекламный девиз, и - видит бог! - это сущая правда.

Эмоциональный заряд сегодняшней истории обеспечила попытка установить на новый ноутбук чистую операционную систему. Нет-нет, речь идет не о преступной Windows XP - боже упаси! Мне всего лишь хотелось украсить SZ650N русской версией Windows Vista Ultimate, любезно предоставленной российским представительством Microsoft старому голубятнику, который на протяжении долгих лет методично гонобобил редмондского гоблина.

Повод для установки чистой ОС (обратите внимание: родной для этого ноутбука) очевиден: желание радикально избавиться от тонн рекламно-софтового мусора, предустановленного Sony.

О мусоре этом я уже рассказывал читателю, но и в страшном сне не мог предположить, что Sony зайдет так далеко в своем стремлении помешать пользователю от оного мусора избавиться. Оглядываясь на поле брани, еще резонирующее криками ярости и раненными стонами, фонтанирующее кровью безвозвратно утерянных нейронов и маразмом бессонной ночи, понимаю, с каким тихим злорадством сведущие люди читали мои бодрые реляции в адрес "аккуратной и грамотной организации службы поддержки Sony", "удобной загрузки фирменных драйверов и утилит", которыми я потчевал читателей пару недель назад, ставя Sony в пример Асусу и Тошибе. "Хех, поживем-увидим!" - потирали ладошки сведущие люди в предвкушении момента, когда у старого голубятника дело действительно дойдет до установки этих самых "аккуратных и грамотных" драйверов и утилит.

И вот время дошло… Забегая вперед, могу лишь сказать, что большего кошмара, чем установка чистой операционной системы на ноутбук Sony, я не видел за девятнадцать лет общения с компьютерами. С этим безысходом не сравнится ничто - ни поиск драйверов для устройств под Windows 95, ни работа с русским языком в Palm OS, ни "кошмар на улице Винтукея" (см. "одноименную" Голубятню то ли пяти-, то ли шестилетней давности). Рядом с Sony вянет все, потому что в остальных

ситуациях не хватало лишь данных - будь то нужного драйвера либо знания, - в случае же с установкой чистой ОС на SZ650N пришлось столкнуться с целенаправленным противодействием производителя любым попыткам отклониться от предписанного им маршрута: хавайте, типа, кипу рекламно-софтверного мусора и не вякайте!

Русская Vista Ultimate встала на чистый отформатированный диск C: моего нового ноутбука как влитая: без малейшего скрипа, проволочки, затруднения. Впрочем, легкость и удобство установки этой ОС я отмечал еще год назад - во время тестирования дорелизной беты. После первого запуска, однако, в диспетчере устройств оказались неопознанными семь железных компонентов ноутбука. Что ж, ситуация вполне стандартная и знакомая любому пользователю мобильного компьютера. Обычно в таком случае мы вставляем диск с набором фирменного программного обеспечения и утилит либо загружаем их на сервере производителя и за пятнадцать минут доводим ноутбук до полной функциональности.

Так бывает - обычно, но не у Sony. Как помнит читатель, никаких дисков с фирменными утилитами к модели SZ650N не прилагается, поэтому отправляемся на сайт компании и загружаем те самые "аккуратные и грамотные файлы". Поначалу бессмысленные названия файлов кажутся нам безобидным чудачеством - устанавливаем все эти TIOOTH-11857500-US.EXE, SOASSL-10555400-US.EXE и т. п. подряд, не замечая подвоха. Но это лишь поначалу…

Итак, загружаем драйверы, устанавливаем на ноутбук и… ничего опять не работает: как было семь железных компонентов, не опознанных операционной системой, так семь и осталось. Что такое? Начинаем рыть по Сети и узнаем, что ад установки чистой ОС на ноутбуки Sony Vaio - хорошо и давно известная пиета на просторах планеты - от болотистой дельты Амазонки до обрывистых берегов Юкона. Об аде этом обломаны сотни тысяч копий, испещрены злыми буквами миллионы страниц форумов и информационных досок.

Не буду заниматься догадками и выяснять, умышленно ли путает Sony ситуацию или в силу гомерического организационного бардака, в общем-то типичного для гигантских компаний, однако реальность такова, что фирменные утилиты и драйверы к различным моделям ноутбуков Vaio всех серий перепутаны, перемешаны, перетасованы с каким-то дьявольским удовольствием. О путанице этой и перетасовке узнаем мы, однако, не сразу, а лишь после того, как, установив утилиты и драйверы и убедившись, что ничего не работает, добираемся на

исходе суток до таинственной инструкции Sony "What is the Windows Vista™ Operating System Clean Install Process?", которая сообщает пользователям, что категорически запрещается устанавливать утилиты и драйверы абы как и в любой последовательности!

Существует, оказывается, строгий алгоритм, что за чем следует:

Sony Shared Library 3.0.00.10180.

Sony Utility 7.0.00.11210.

Setting Utility Series 2.0.00.11230 и так далее - 42 пункта.

Здесь-то и оказывается, что половина перечисленных ключевых утилит, без которых невозможно нормальное функционирование ноутбука, элементарно отсутствует в списке программ для вашей конкретной модели, и где ее искать и брать - совершенно непонятно.

Читатели помнят, что модель моего ноутбука изготовлена специально для американского рынка, поэтому в Эрэфии считается "серой" и, следовательно, никак не поддерживается. Так вот: слава богу, что не поддерживается, потому что на американском сервере Sony есть хоть какие-то утилиты и драйверы, тогда как на российском… да что там: полюбуйтесь сами на скриншот страницы технической поддержки модели ноутбука, аналогичной моему SZ650N.

Видите внизу жалкий огрызок (Vaio Smart Network 1.0)? Врубаетесь в смысл послания? Правильно: "Нефиг что-то менять и куда-то лазить! Купил, ламер, за три штуки баксов черный ящик и радуйся жизни!"

Короче, в ситуации, когда на сайте производителя отсутствует полноценная поддержка фирменных утилит и драйверов, не остается ничего, кроме как часами собирать по крупицам информацию на разрозненных форумах, компилировать десятки противоречащих друг другу алгоритмов, загружать первый драйвер - по линку одной модели, второй - по линку другой модели… И так далее - до тех самых пор, пока все наконец-то не установится и вместо семи неработающих железных компонентов в диспетчере устройств ОС не останется… два!

Да-да, именно два неопознанных гаджета - встроенная веб-камера и адаптер для чтения карт SD/MMC - явились высшим моим достижением по результатам трех чуть ли не круглосуточных усилий по установке чистой Windows Vista Ultimate на ноутбук Sony Vaio VGN-SZ650N/C. Ну плюс еще мелочь типа периодического выскакивания на экран сообщения о том, что установленная аккумуляторная батарея не совместима с

данной моделью компьютера, поэтому следует незамедлительно нажать на кнопку ОК, чтобы перейти в спящий режим, затем вытащить аккумуляторную батарею и вставить снова. Стоит ли говорить, что никакие вытаскивания не помогают, потому что дело вовсе не в батарее, а в несовместимости утилиты Sony Battery Check с русской версий Windows Vista. По крайней мере так написано на одном из форумов, а уж какова подлинная причина безобразия - никому неведомо.

На исходе дня наступила апатия, и внимание на форумах все больше стали привлекать реплики вроде: "Дополнительные приблуды типа дактилоскопического сенсора и камеры в общем-то не нужны - это скорее дань моде, а в повседневной жизни я ими не пользуюсь".

Мне, к сожалению, приходится пользоваться веб-камерой ежедневно и по многу раз, так что пришлось откатываться к предустановленному пакету, а затем удалять софтверно-рекламный мусор с максимально возможной тщательностью. Для этого задействовал программу Your Uninstaller 2006 Pro, о которой, кстати, никогда не писал в "Голубятнях", а посему, пользуясь случаем, представляю читателям. Изюминка Your Uninstaller: программа сначала внимательно следит за процессом стандартной системной деинсталляции, а затем самостоятельно шерстит реестр, удаляя мусор, остающийся после штатной процедуры. В том, что этот мусор остается, причем в ужасных количествах, можно не сомневаться: даже малюсенькая утилитка для КПК - pTravel Alarm - оставила после удаления двадцать ключей в реестре. Монстры типа MS Office Small Business Edition, триал которого предустановлен на ноутбуке зачем-то вместе с MS Works, оставляют до трехсот "хвостов"!

Опять я вернулся к Windows Vista Business, опять удалил рекламно-триальный мусор и опять с горечью констатировал, что система еле ползает, так, видимо, и не оправившись после изначального надругательства. И тогда я взбунтовался: ну должен же быть, черт возьми, выход из положения! Выход яркий, выразительный, эвристический - подобно гениальнейшему оживлению брикнутых сониевских ЗЫЗ с помощью аккумуляторной батарейки, описанному недавно в "Голубятне". Однако вместо выхода - лишь заунывно-тупая парадигма, повсеместно адаптированная на россиянских форумах: установил чистую ОС и ковыряйся с драйверами до потери сознания, собирай шматки по сусекам, компилируй, переставляй с места на место…

Вам это ничего не напоминает? А мне вот напоминает - анекдот про бананы на пальме и милиционера: "Может, палкой

сбить попробуете?" - "Какая, в задницу, палка?! Трясти нужно дерево, трясти!" Вот и трясут любители ноутбуков Vaio безнадежную пальму Sony, камлают неделями, потом хвастаются достижениями. Убогими. Почему так? Да потому, что интонации на россиянских форумах задают гоблины - узколобые рыцари паяльника и Си-плюс-плюс, чуждые полета фантазии, пришибленные квадратно-гнездовым мышлением.

И тогда, движимый интуицией, я обратил взор на Пиндустан, высмеянный завидующим миром за чудаковатость и прямолинейность, однако созидающий 90% мирового ноу-хау. И что же? Пятнадцать минут целенаправленных поисков на форуме notebookreview.com хватило для обнаружения ГЕНИАЛЬНОГО алгоритма, позволяющего вклиниться в автоматический процесс инсталляции софта на ноутбук в момент ПОСЛЕ установки операционной системы всех необходимых драйверов Sony и ДО установки софтверно-рекламного мусора! Алгоритм этот был успешно протестирован автором на моделях серий CR, SZ, FZ, AR и TZ, я же получил идеально чистую Windows Vista со всеми действующими драйверами на Vaio VGN-SZ650N/C всего за пятнадцать минут! Как?! Узнаете через неделю!

P.S. Гениальный алгоритм на форуме notebookreview.com был представлен пользователем по имени Oleg, родом из Украины. Как видите, эвристика по-прежнему является венцом нашей цивилизации, хотя и обретает творческое воплощение на форумах Пиндустана. В этом, собственно, и кроется адекватное восприятие моей филиппики в адрес отечественных форумов: проблема не в дефиците гениальности у русских людей, а в ефрейторской субкультуре гоблинов, цветущей гнилым цветом на россиянских форумах и всякую эвристику удушающих. Потому-то кудесник Олег и поместил свой пост на notebookreview.com.

опыты: Tor — круговая порука

Автор: Филипп Казаков

Сегодня, 19 октября 2007 года, я зашел на Yandex.ru, а затем на Google.ru, и ввел простой запрос: "tor". В первых строках результатов оказалось три ссылки по существу вопроса, одна из которых вела на официальный сайт проекта, две другие - на wiki-статьи, но не нашлось ни одной статьи из СМИ. Это меня и возмутило: как же так, почему население Российской Федерации не знакомят с одной из самых интенсивно развивающихся технологий анонимизации в Сети? Случайно ли это?

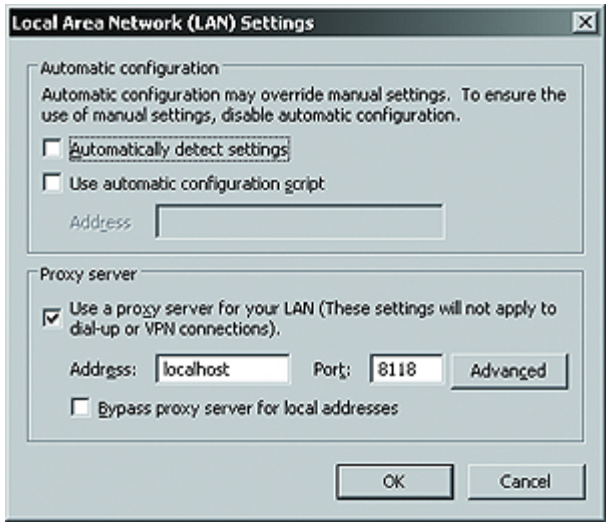
Сэтой технологией я познакомился полгода назад, причем совершенно случайно, так как Tor загадочным образом не пользуется популярностью в Рунете. На самом деле "КТ" была бы не "КТ", если б не написала о Tor'е еще два с половиной года назад ("Одежки с застежками"). Тогда, в 2005-м, Tor был интересным и перспективным проектом, но довольно неудобным в практическом плане. Впрочем, разработчики не сидели сложа руки, и сегодня Tor - комфортный и простой в применении анонимизатор интернет-соединений, пользоваться которым может кто угодно.

О Tor-сети подробно рассказано в вышеупомянутой статье "Одежки с застежками", так что сегодня я ограничусь самым общим описанием технологии ее работы, просто чтобы ввести читателя в курс дела. Tor - это распределенная сеть анонимизаторов, она состоит из множества tor-серверов, запущенных и поддерживаемых на тысячах компьютеров добровольцев по всему миру - простых пользователей сети. Любой желающий настраивает на своем компьютере специальный софт (бесплатный, с открытым исходным кодом!), позволяющий использовать всю tor-сеть как свой proxy-сервер. При этом маршрутизация запросов проходит через несколько случайным образом выбранных tor-серверов, да еще и меняется каждые десять минут. По мере путешествия от пользователя к серверу и обратно трафик подвергается многослойному асимметричному шифрованию. Конечно, каждый сервер цепочки может узнать, с какого IP он получил зашифрованные данные и кому он их дальше передаст, но сам трафик и конечный адресат пакетов остаются тайной для всех, кроме оконечного сервера цепочки.

Tor-сеть вызывает ассоциации с p2p-сетями, особенно с протоколом ed2k. Главное сходство - идеологическое: каждый участник вносит свой вклад в создание и поддержку общего дела

(по возможности), а также безвозмездно пользуется благами его роста и процветания (по потребности). Как и ed2k, Tor "страдает" легкой централизацией: список активных серверов сети в начале работы клиент скачивает с основного, заранее известного сервера компании. Впрочем, так как вся сеть пока абсолютно легальна (по крайней мере с точки зрения демократических государств), вряд ли ее ожидают потрясения, сравнимые с недавними бедами ed2k [Напомню, что в середине сентября правозащитные организации закрыли все основные серверы ed2k-сети, частично заменив их одноименными фальшивками].

Чем больше пользователей и tor-серверов находится в tor-сети, тем выше анонимность соединений: меньше вероятность того, что на конец маршрута попадет "вражеский" сервер, стремящийся украсть ваши данные. Вероятность подобного стечения обстоятельств и так близка к нулю, если, конечно, вы не международный террорист, за которым идет охота всем миром. Очевидно, что жизнеспособность tor-сети зиждется на добровольных участниках, "поднимающих" tor-серверы на своих домашних машинах. Разработчики это отлично понимают, поэтому за прошедшее с момента выхода "Одежек..." время сделали огромный шаг в направлении упрощения работы с системой. Никакие командные строки, ini- и config-файлы больше не омрачат ваше знакомство с сетью. Все, что нужно для работы с Tor под Windows, - это единый инсталляционный пакет, содержащий необходимые программы (русскоязычная сборка). Процесс установки не требует никаких специальных знаний. В сборку включены три программы: Tor, Vidalia и Privoxy. Консольный tor.exe - это и есть основное звено комплекса, общающееся с внешним миром. Vidalia - просто графическая оболочка для tor.exe, обеспечивающая его взаимодействие с вами. Наконец, Privoxy - суть локальный proxy-сервер, предназначенный для связи вашего веб-приложения и Tor'a. Он анализирует активность браузера и мягко напоминает ему "Не болтай!", вырезая всю служебную информацию, могущую послужить вашим идентификатором. Заодно Privoxy подрезает некоторый процент баннеров, экономя трафик. Налицо классическая модульная система, свойственная открытому программному обеспечению.



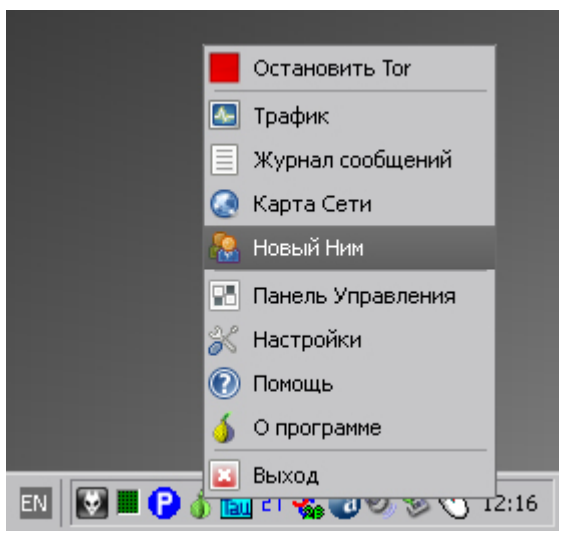
После установки вся связка начинает нормально работать, что неоднократно проверялось мною на разных Windows-машинах. Для начала работы осталось настроить ваш браузер на конспиративный лад. Если это Internet Explorer, просто задайте в настройках соединения proxy-сервер "localhost" (то есть вашу машину, иначе говоря, Privoxy) и порт 8118 [1].

Для свободного и открытого Firefox, к которому tor-сообщество относится не в пример благосклоннее, чем к IE, существует удобное расширение Torbutton. После его установки в строке состояния появляется кнопка, при клике на которую Firefox мгновенно "торизуется".

Попав в сети

Теперь все готово. Для проверки зайдите, например, на сайт www.cmyip.com: "My country is United States, My city is Red Oak". Красота! Виртуальная маска успешно надета, ведь на самом деле со своего московского кресла я даже не вставал! Чтобы немедленно сменить маршрут подключения, достаточно в трей-панели выбрать пункт "Новый Ним" по правому клику на значке Vidalia [2]. Алле-оп, и я уже в Париже! [Программа не позволяет выбирать конкретное будущее виртуальное местоположение, оконечный сервер будет задан случайным образом, но процедуру можно повторить несколько раз для достижения желаемого результата. - Прим. ред.] Google.com по умолчанию перестает предлагать русскоязычный интерфейс, реклама на сайтах зачастую переводится на совсем незнакомые языки, да и предлагает непонятные вещи. Став "гражданином Мира",

придется кое-чем поступиться. Под Tor'ом сайты открываются совсем не так шустро, как при прямом подключении. Причем не так сужается канал, как увеличивается время ожидания ответа. Если "туннель" совсем "забился", всегда можно переключиться на другую цепочку серверов. Аппаратные требования комплекса очень скромные - вся троица приложений занимает около сорока мегабайт на диске и требует около десяти секунд усилий CPU Intel E4300 на час серфинга. Кроме своего основного предназначения, Tor - отличное средство от мелких сетевых напастей. Если какой-то сайт не открывается или глючит, попробуйте достучаться до него через Tor. Вполне возможно, что проблемы вовсе не на самом сайте, а где-то в цепочке "сайт-провайдер-клиент", а с другой стороны (например, из Бразилии) узел откроется нормально. Наконец, помните, что сам по себе Tor не является универсальной защитой - это всего лишь удобный и надежный сервис. Остальная забота о безопасности и анонимности целиком остается на вас (см. врезку на следующей странице).



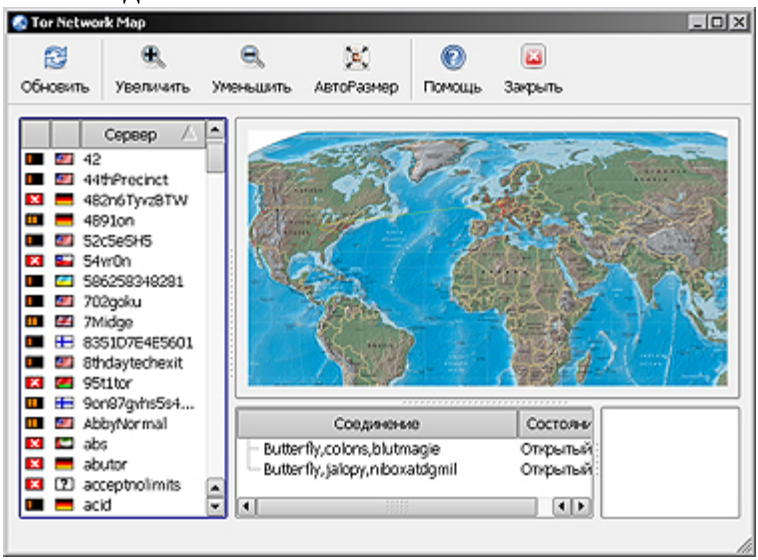
Теоретически Tor может анонимизировать любые TCP-подключения. Сообщество разработчиков пока не рекомендует использовать Tor для p2p-сетей, так как tor-сеть еще не готова к огромному трафику, генерируемому пиринговой активностью. Признавая справедливость рекомендации, я все же не сумел унять любопытство и провел эксперимент с анонимизацией torrent-трафика. Для этого использовались µTorrent 1.6, настроенный на работу через Privoxy, и один из русскоязычных трекеров. Как и следовало ожидать, все подключения получили статус LowID (невозможность прямого подключения), но при этом обмен

данными продолжался, причем скорость скачивания достигла солидных 250 Кбайт/с!

Интересные подробности о работе сети можно почерпнуть из главного меню Vidalia [3].

Кнопка "Просмотреть Сеть" вызывает карту Земли, где красными точками отмечены очаги анонимизации, то есть активные tor-серверы. Желтые и зеленые прямые соединяют те из них, которые в данный момент обслуживают ваш "туннель". Слева располагается полный список серверов сети, каждый из них сопровождается кратким описанием [4]. По анализу времени непрерывной работы и скорости подключения первой сотни серверов я осмелюсь грубо прикинуть, что "частников" в tor-предприятии примерно в 2–2,5 раза больше, чем "настоящих" серверов. Некоторые энтузиасты успешно используют для серверов компьютеры на базе процессоров i386, но, конечно, не под Windows. Есть и еще несколько любопытных наблюдений: в России всего четыре-пять очагов сопро… анонимизации, в которых на момент написания статьи работало всего двадцать серверов [На самом деле числа чуть большие, так как для определения местоположения серверов Tor использует таблицы IP-адресов с сайта geoip.vidalia-project.net. Информация в них не всегда актуальна, и местоположение многих IP-адресов помечается как неизвестное. Так, моего сервера в российских списках нет, хотя по имени его можно найти]. Шестнадцать из них в Москве, по одному в Питере и Тюмени и два в Пензе (анонимный привет пензенским жителям!). Больше всех озабочены проблемами анонимности жители Германии и США, их

доля в общем котле самая большая, и российскую превышает многократно. В Китае тоже немало серверов, да только большая их часть в дауне или едва работает. Австралийцев мало волнуют все эти проблемы - вместе с новозеландцами они взрастили с десяток tor'оводов.



Паучьи игры: плетем сети сами

Поскольку большая часть населения России борется за увеличение ВВП, за спортивные победы, сражается с пьянством, преодолевает демографический кризис и занимается прочими не менее увлекательными делами, нет ничего удивительного, что вопросам Свободы Слова и анонимности вообще, а в Интернете в частности, внимания уделяется маловато. Но все-таки обидно, согласитесь: в нашей "самой-самой" стране всего двадцать серверов! Ну даже если б пятьдесят, все равно обидно! Пока tor-серверов у нас не много, каждый постоянно подключенный к Интернету россиянин может без особых усилий заметно (на пару процентов) повысить tor'изацию всей страны, несмотря на ее необъятность. Если вы обратили внимание на приведенный скриншот интерфейса Vidalia, то не могли не заметить большую кнопку "Настроить сервер". Все очень просто: нажимаем кнопку, ставим в открывшемся окне галку "Режим сервера", указываем любое имя, контактный e-mail для получения новостей о критических обновлениях, выбираем порты (их надо "открыть" в роутере или в софтовом файрволле). Галку "Зеркалить Directory" ставим только если готовы выделить широкий канал для tor-сети. В следующей закладке выбираем ограничение трафика (в обе

стороны). Можно задать не только максимальное мгновенное значение, но и среднее по времени на тот случай, если ваш месячный трафик лимитирован. Минимально допустимая ширина - 20 Кбайт/с. Синхронизируете ваши Windows-часы с общемировым временем, и вот собственно вся настройка. Сервер поднимется не сразу, а минут через десять-двадцать. За его состоянием можно следить по "Журналу сообщений" и по активности "Трафика".

К сожалению, я не успел рассказать о многих других интересных возможностях Tor'а - например, о скрытых сервисах. Остается надеяться, что кого-нибудь из читателей, как и меня, заинтересует эта технология, что со временем приведет к ее гораздо более широкому распространению.

Tor - не шапка-невидимка

Помните, что Tor - не волшебная шапка-невидимка, надев которую вы вдруг исчезнете. Это лишь один из многих инструментов (в их числе должна быть и голова пользователя!), помогающий соблюдать анонимность. Как вы помните, последний сервер цепи анонимизаторов имеет доступ к информации пользователя в открытом виде. Информацию можно защитить от несанкционированного доступа со стороны этого сервера, однако тут необходимо использовать альтернативные технологии - SSL-протокол или другие защищенные соединения (подробнее см., например, ru.wikibooks.org/wiki/Защита_конфиденциальных_данных_и_анонимность_в_интернете). Кстати, на странице загрузки дистрибутива Tor'а висит огромное предупреждение об этом и других ограничениях функциональности сети, а также базовые рекомендации по их преодолению. К несчастью, масса пользователей пропускает эти рекомендации мимо ушей (глаз). И напрасно.

Месяц назад об ограничениях Tor'а напомнил Дан Эгерстад (Dan Egerstad), шведский специалист по сетевой безопасности. Исследуя сеть, он "поднял" пять собственных tor-серверов. Так как общее количество серверов в tor-сети пока не слишком велико, эта пятерка оказалась заметна в общем трафике. Как выяснилось, 90% пользователей Tor'а не используют каких бы то ни было дополнительных средств шифрования. Периодически серверам Дана доводилось работать выходными звеньями "туннеля", что позволяло собирать проходящий через них нешифрованый трафик. Всего два месяца понадобилось Дану для того, чтобы вычленить из собранных данных логины и пароли от более чем

1500 e-mail-аккаунтов самых разных tor'овцев, вплоть до правительственных служащих и представителей крупных компаний. Тщетно пытаясь привлечь внимание к результатам своего исследования, Дан в конце концов опубликовал данные по ста аккаунтам в Интернете. Вот тут-то его и заметили!

Охотники на инфузорий

Автор: Юрий Смирнов smir@kvidex.ru

Получение гонорара за опубликованные материалы - дело тонкое. Одно издательство на карточку денежку кидает, другое по факту сдачи статьи платит... Когда я получил деньги за опубликованные летом в "КТ" материалы, передо мной встала труднейшая задача - на что же их потратить? Ведь деньги, как мед, - они если есть, то их сразу нет.

В голову пришла мысль о микроскопе "Юннат" (см. "КТ" #703), который был подарен нашему программисту. Полез я на микроскопный сайт, чтобы провести микромаркетинг.

"Держаться надо в русле политики партии и правительства", - с гордостью думал я, изучая микродевайсы. Для нанотехнологий разрешение "Юнната" было явно маловато. По соотношению цена/характеристики больше понравился "Микромед-Р1", для него было заявлено максимальное увеличение 1600х. Стоила игрушка разумно - всего 7,7 тысячи рублей. До кучи пришлось заказать к нему камеру посерьезнее, с максимальным разрешением 3 мегапиксела - MYscope 300M.

В прошлый раз, когда я заказывал "Юнната", мне привезли в подарок от фирмы коврик для мыши, на котором было написано, что его обладатель может получить скидку 7%. Никогда не доверял такой халяве, но в этот раз сработало. Делая заказ по телефону, я представился, как обладатель коврика, и менеджер без лишних вопросов скинул мне 7%.

Курьер привез заказ, как всегда, к концу рабочего дня, и микроскоп мы с программистом начали тестировать только на следующий день. Меня больше всего волновал вопрос, подойдет к нему камера или нет. Воткнуть камеру-окуляр оказалось так же просто, как и в прошлый раз в "Юннат". По размерам MYscope 300M (по другой версии она называется DCM 300) чуть больше DCM35, подключается она к компьютеру также через USB-порт. Драйвер установился одним нажатием кнопки, так же просто была инсталлирована программка ScopePhoto. Вся система как-то заработала.

Микроскоп "Микромед-Р1"

Монокулярный микроскоп с револьверной головкой
Увеличение 40–1600х
Объективы-ахроматы 4х0,1; 10х0,25; 40х0,65; 100х1,25
Окуляры 10х18; 16х15
Конденсор Аббе с апертурой 1,25
Двухкоординатный предметный столик 110х120 мм
Встроенный осветитель (источник света - лампа 6 В, 20 Вт)

Препаратов под рукой не оказалось. У коллеги на столе был найден волос, который мы изучили, меняя объективы (увеличение). До 800х все подстраивалось нормально, но при максимальном увеличении отрегулировать резкость мы не смогли. Четкость изображения была потрясающая, даже по сравнению с "Юннатом". Наверное, эффект увеличения четкости дает наличие в конструкции микроскопа конденсора Аббе, благодаря которому препарат подсвечивается лучше, чем в "Юннате". С виду конденсор напомнил мне аналогичное устройство от старого фотоувеличителя, да и работает он по тому же принципу.

Структура волоса при увеличении 200х и больше походит на только что спиленное бревно - поверхность при сильном увеличении напоминает кору дерева. За обедом мы увлеченно обсуждали вопрос, кому же может принадлежать этот волос со стола. Согласитесь, что по этому поводу может возникнуть много интересных предположений. Но микроскоп надо было уносить домой, и сделать сравнительный анализ волос всех сотрудников мы не успели.

Дома, внимательно изучив инструкцию, я понял, почему мы не могли настроить изображение на максимальном разрешении. В инструкции черным по белому прописано: "Объективы 40 и 100 имеют пружинящую оправу для предохранения от механического

повреждения фронтальной линзы и объекта. Объектив 100х рассчитан на работу с масляной иммерсией". Слово "иммерсия" было мне незнакомо, но интуитивно (с подачи жены) я просек, что объектив (линза) смачивается очищенным маслом, которое входит в комплект микроскопа. При подведении объектива (линзы) к объекту возможно соприкосновение с покровным стеклом, и на этот случай масло предохраняет линзу. Кроме того, масляная прослойка и сама играет роль линзы, изменяя фокусное расстояние объектива.

Принцип наводки на резкость в "Микромеде" не такой, как в китайских игрушках и "Юннате". Если в "Юннате" ползает вверх-вниз трубка микроскопа, то в "Микромеде" двигается предметный столик, причем в трех плоскостях, а трубка жестко закреплена на металлическом штативе.

Предметный столик двигается вверх-вниз двумя ручками: грубой фокусировки и точной. Это очень удобно при работе с большим разрешением (от 800х), стол подводится к объективу ручкой грубой фокусировки, а непосредственно настройка на резкость осуществляется уже ручкой точной фокусировки. Двумя другими ручками предметный столик можно перемещать вправо-влево и вперед-назад.

Механизм подсветки препарата в этом девайсе также сильно отличается от предыдущей рассмотренной модели. Это 20-ваттная лампочка накаливания, система линз (упомянутый выше конденсор Аббе) и ручная диафрагма. Диафрагма позволяет плавно менять освещенность объекта. Небольшой минус все-таки есть: микроскоп довольно сильно греется, и есть ощущение, что лампочку подсветки придется часто менять (в комплект входит запасная).

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ DCM 300

Чувствительный элемент 3 млн. пикселов, 1/2” CMOS

Максимальное разрешение 2048x1536

Размер просмотра видео 800x600, 1024x768, 1280x1024, 1600x1200, 2048x1536

Спектральный диапазон 380–1000 нм

Способ экспозиции ERS (электронная моментальная фотография)

Контроль экспозиции авто/ручной

Баланс белого авто/ручной

Интерфейс USB 2.0

Программные регулировки размер изображения, яркость, время выдержки

Диапазон рабочих температур –10… + 50 ˚C

Поле зрения круг диаметром 18 мм

Формат изображения BMP, TIFF, JPG, PICT, SFTL и др.

Программное обеспечение драйвер, программа ScopePhoto

Все воскресенье жена убила на новую игрушку. Особым достижением была видео- и фотосъемка инфузорий-туфелек, которых удалось прикормить на кисломолочных бактериях. Изображение водоросли Ричи при большом увеличении напомнило мне кадры из фантастического фильма. До кучи жене удалось опять наловить в аквариуме жгутиковых (как правильно заметил г-н Шошин в своем письме, это не жгутиковые, а кругоресничные сувойки) и снять фильм из их жизни. Видео вы можете посмотреть в блоге "КТ" (inside.computerra.ru). Наблюдать инфузорий и бактерий было интересно, но мне захотелось сравнить качество печати фотографии в журнале с газетным качеством, поскольку мои фотки публиковались и в "КТ", и в еженедельнике "Народный совет". Я препарировал оба издания (вырезал маленькие квадратики) и засунул под микроскоп.

Результаты микроизучения медиарынка вы можете увидеть на фото - качество бумаги сильно отличается (ни одно из изданий в ходе эксперимента серьезно не пострадало).

После этих съемок с увеличением до 800х мы решили перейти на максимальное увеличение, и тут нас ждал небольшой сюрприз. Микроскоп комплектуется двумя окулярами с коэффициентом увеличения 10х и 16х. Коэффициенты увеличения окуляра и объектива перемножаются, то есть при окуляре 10х и объективе 4х линейное увеличение составляет 40х. При окуляре 16х и объективе 100х мы получаем увеличение 1600х, как и было объявлено в рекламе. Но камера-окуляр обладала коэффициентом 20х, то есть максимальное увеличение составило 2000х! Вот это и было приятным сюрпризом.

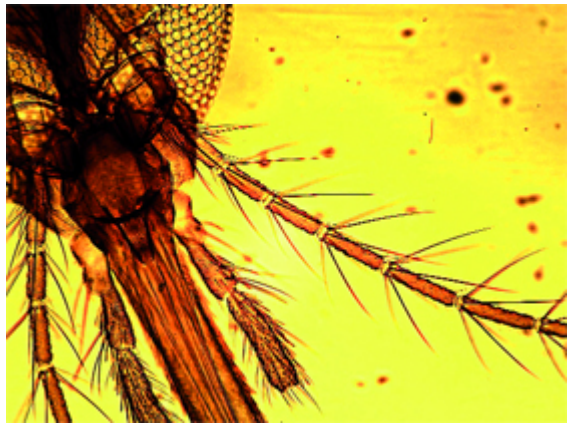
Тут пришла идея изучить под микроскопом кровь. Моя дочь Катя недавно сдавала кровь на диспансеризации, и первой сдать кровь на исследование я предложил ей. Дочь стала активно протестовать, а я запугивать ребенка. Пока мы с ней играли в доктора, жена уже организовала сеанс просмотра собственной крови. Для работы с таким увеличением пришлось смачивать объектив маслом, без которого микроскоп не удавалось настроить на резкость - на экране компа лишь размытое красное пятно.

Камера-окуляр позволяет снимать видеоролики с разрешением 640х480, но в программе есть опция, которая позволяла делать серию фоток (несколько кадров в секунду) уже с разрешением 1600х1200. Такую серию, в принципе, можно склеить в ролик и получить видео с весьма приличным разрешением.

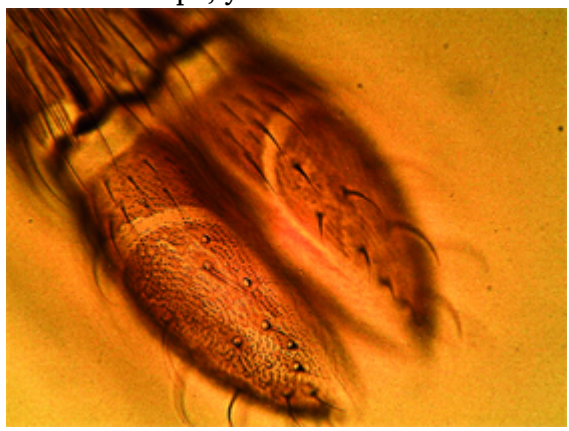
В заключение хочу обратить внимание читателей, что производитель этого микроскопа - отечественное предприятие ООО "Наблюдательные приборы" из Питера. В паспорте все по-взрослому - стоит оригинальная роспись представителя ОТК, штамп завода, заводской номер. Давненько я такого не видывал! Приятно, что можно купить хоть что-то отечественного производства, причем хорошего качества.

Вот что видно в окуляре

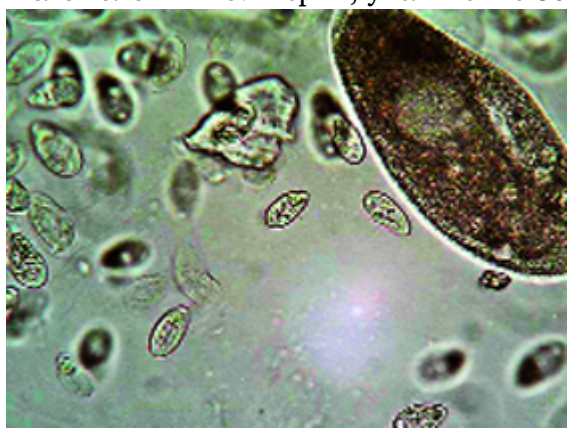
1. Часть головы страшного монстра-комара, увеличение 80х



2. Конец хобота комара, увеличение 200х

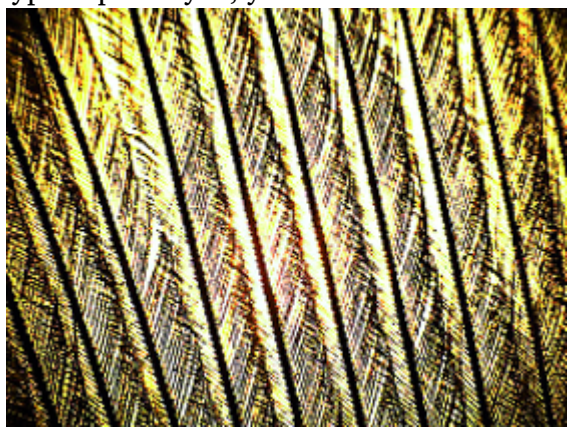


3. А вот и "тапочка" (туфелька) собственной персоной, охотится на кисломолочных бактерий, увеличение 800х

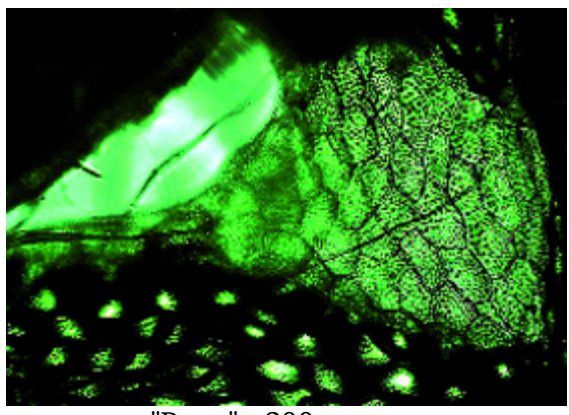


4. Картина "Заход солнца". Перо голубя, увеличение 80х

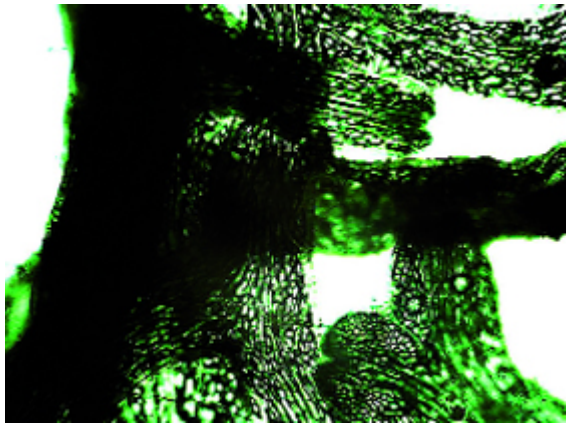
5. Структура пера голубя, увеличение 200х



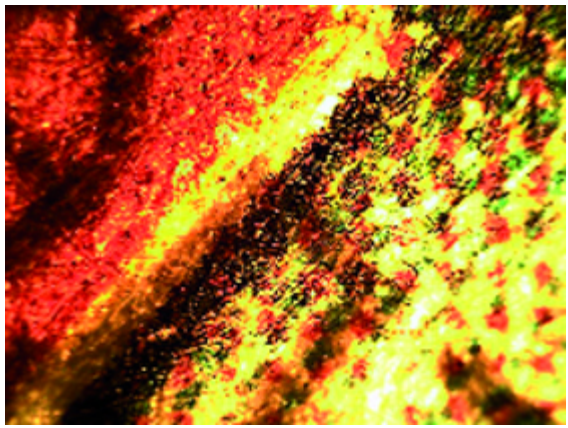
6. "Страшная" водоросль "Ричи" из аквариума, увеличение 800х

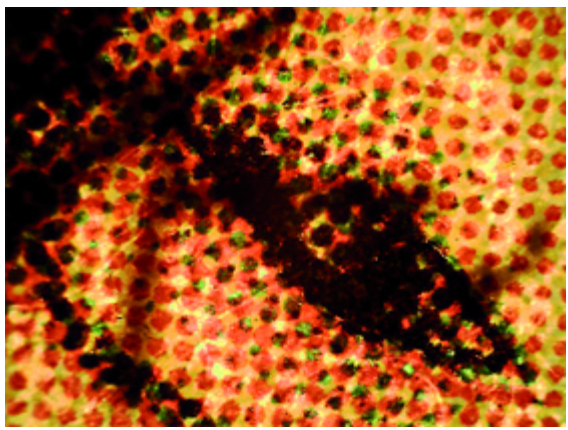


7. Та же водоросль "Ричи" - 200х

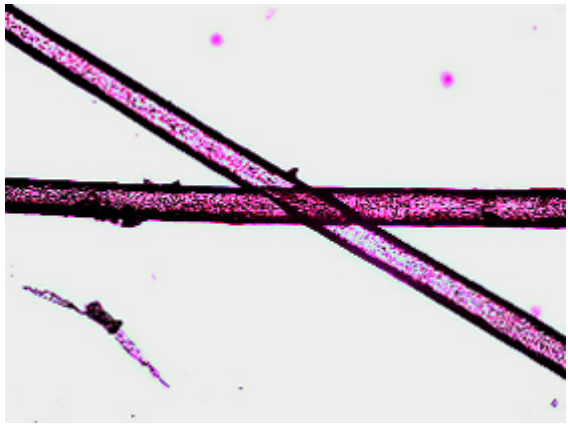


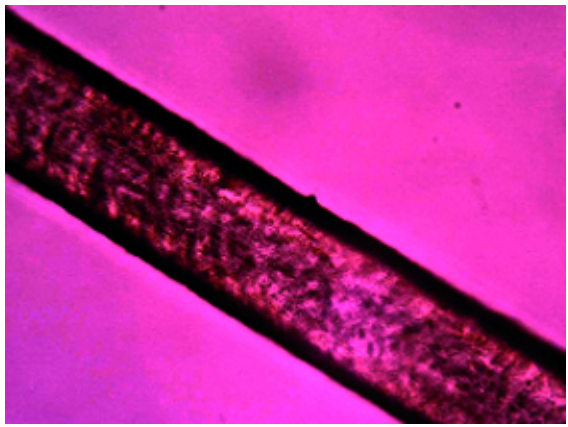
8,9. Сравнив микрофото "Народного совета" и "КТ", можно увидеть, чем газетная печать отличается от журнальной



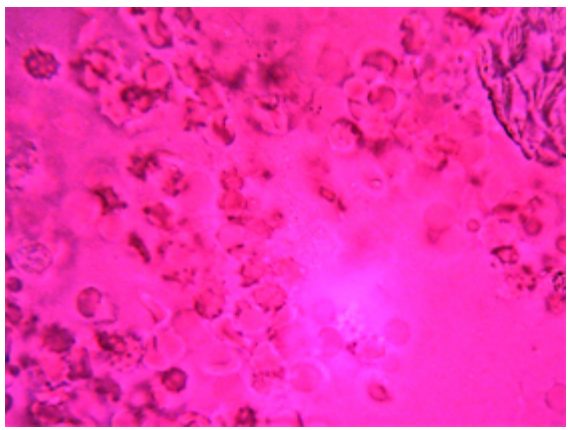


10,11. "Бревно" на снимке - мой волос, извините, с ноги, увеличение на втором снимке - 800х





12. Это не кадр из фильма "Внутреннее пространство", а кровь при увеличении 2000х. Изображение тонировано программно в ScopePhoto



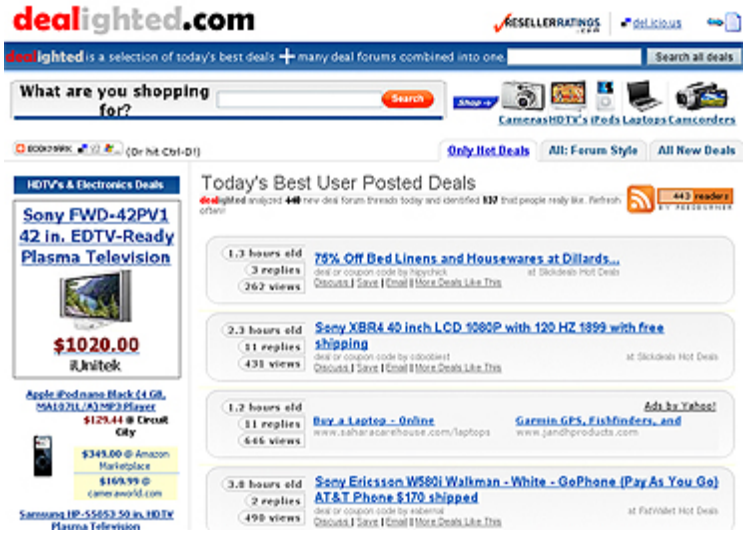
P.S. Моему ребенку в школе показывали бактерий, для чего приезжала специально обученная тетенька с ноутом и проектором, заказанная школой за отдельные деньги. Меня сей

факт слегка задел. Если вы, уважаемые читатели, захотите заглянуть в микромир или показать своему ребенку, как выглядит бактерия, сходите на сайт "КТ" по приведенной выше ссылке. А можете даже организовать собственный микробизнес - качните фотки и ролики, почитайте учебник по биологии, после чего можете спокойно зарабатывать деньги, объезжая школы и демонстрируя детям прелести микромира.

софтерра: Webология

Автор: Илья Шпаньков

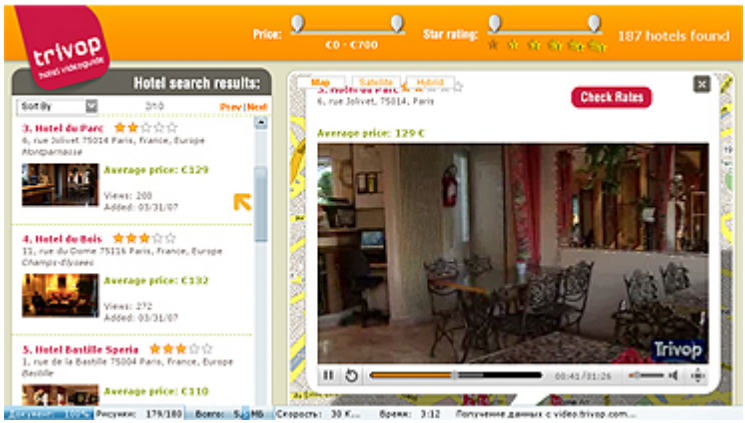
За реальные деньги



Адрес www.dealighted.com
Интерфейс английский
поддерживается уведомление по e-mail

Я всегда подозревал, что, приобретая цифровые устройства в магазине, мы переплачиваем немалые суммы, но реальный масштаб неоправданных расходов при покупке, например, телевизора можно почувствовать, заглянув на онлайновый портал Dealighted.com. Здесь скрупулезно собирается информация о рекламных акциях, скидках, купонах и прочих бонусных прелестях современной системы продаж дорогих товаров. Даже если продавец предлагает всего лишь бесплатную доставку покупки вам домой, это предложение уже пригодно для размещения на страницах портала. Как и положено подобным ресурсам, все позиции подробно описаны и снабжены рейтинговой оценкой, благодаря которой можно выбрать самые выгодные. Кстати, торговые компании тоже знают о Dealighted.com и постоянно размещают на нем свои предложения. К сожалению, дороговизна доставки в Россию нередко съедает возможную экономию.

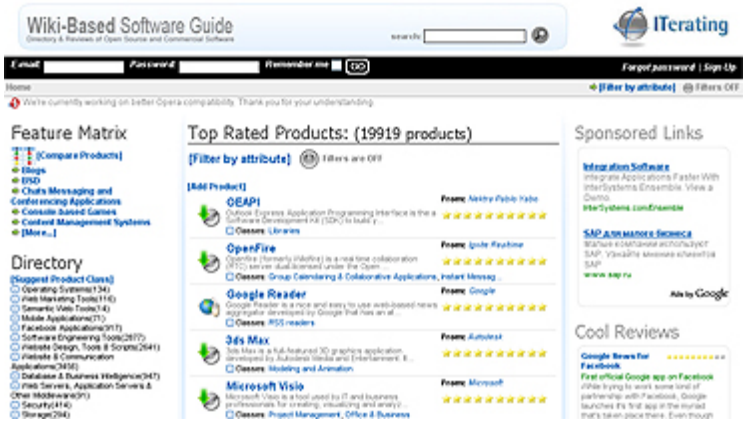
Лучше один раз увидеть



Адрес www.trivop.com
Интерфейс английский
требуется флэш-плагин

Для людей, часто разъезжающих по странам и континентам, немаловажное значение имеет то, в каком отеле остановиться: все-таки пусть на время, но он станет домом, и никому не безразлично, каково будет это жилище. Рекомендуем путешественникам заглянуть на онлайновый портал Trivop - здесь собраны видеоролики, отснятые в различных (в основном европейских) отелях и наглядно демонстрирующие, что вас ждет при выборе той или иной гостиницы. Конечно, как и для фотографии, так и для видеосъемки можно навести марафет даже в самой никудышной ночлежке, но все-таки впечатление после просмотра окажется максимально приближенным к реальности. Отдельное спасибо можно сказать создателям портала за подробный план расположения отеля, позволяющий легко ориентироваться в незнакомом городе.

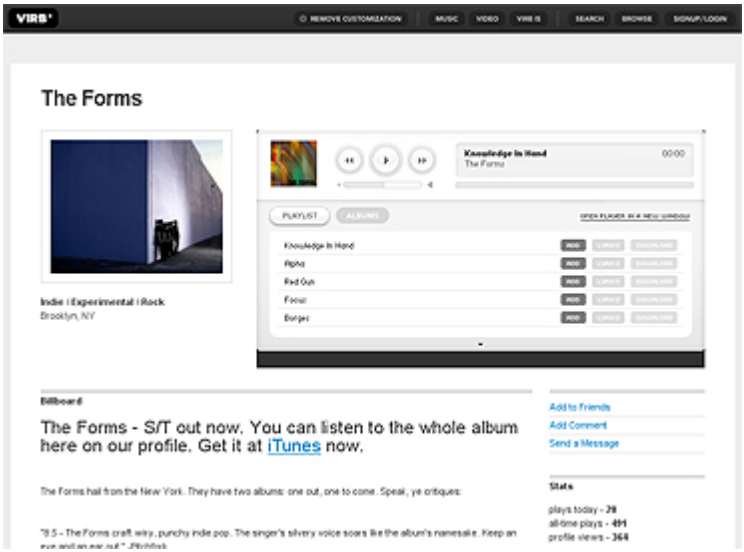
Энциклопедия софта своими руками



Адрес www.iterating.com
Интерфейс английский
кириллица не поддерживается

Мы используем в работе десятки, если не сотни компьютерных программ и в итоге приобретаем опыт, который может оказаться полезным тем, кто ищет программы, максимально отвечающие его запросам. Но как поделиться своим знанием? Очень просто - зарегистрироваться на онлайновом ресурсе Iterating и рассказать о любимых приложениях и операционных системах. Ресурс построен в виде вики: каждый посетитель может высказать свое мнение и внести поправки в уже существующие статьи. Отметим довольно продвинутую систему рейтинга, позволяющую оценивать софт по нескольким типичным параметрам. В итоге получается средняя оценка программы, весьма близкая к реальной. Но и это не все: при желании данные можно использовать для сравнительного анализа однотипных приложений. В настоящее время база сервиса насчитывает более 10 тысяч статей.

Мультимедийный комбайн



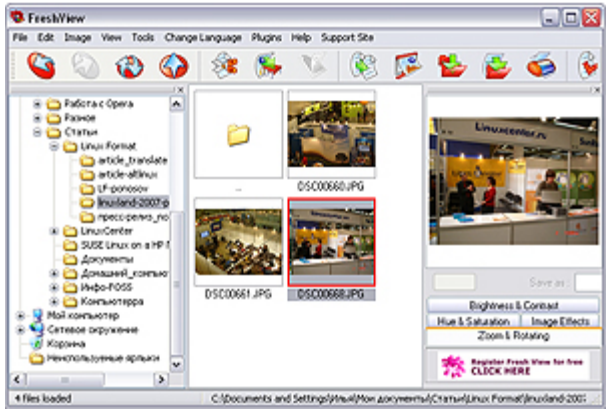
Адрес www.virb.com
Интерфейс английский
требуется флэш-плагин

Почему популярны многофункциональные устройства? Потому, что удобно - все функции находятся под рукой. Зачем же тогда заводить массу учетных записей на различных онлайновых сервисах для хранения видео, музыки, изображений? Не лучше ли воспользоваться сервисом Virb, который позволяет хранить все свои мультимедийные реликвии в одном месте. По сути, это обычная социальная сеть для творческих людей, где можно делиться новыми идеями, заявлять о себе миру и публиковать свои художественные изыскания. Впрочем, ресурс придется по душе не только творческим личностям; сервис Virb станет своего рода зеркалом состояния современной культуры для тех, кто профессионально занимается изучением столь глобальных вопросов. Пожалуй, единственное, чего не хватает порталу, это более наглядной классификации размещаемых материалов и поиска по заданным фильтрам и критериям.

Софтерринки

Автор: Илья Шпаньков

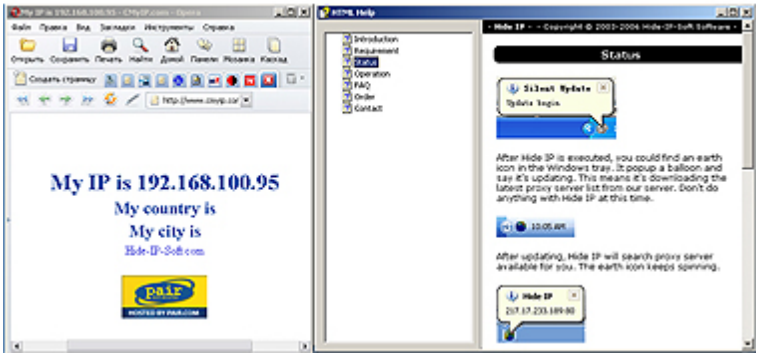
Свежий взгляд



ОС Windows
Адрес www.freshdevices.com
Версия 7.34
Размер 2,2 Мбайт
Интерфейс многоязычный (русский не поддерживается)
Цена бесплатно
Лицензия проприетарная (Freeware)

Для того, чтобы понять, каково содержимое того или иного медиафайла, совсем не обязательно открывать этот файл в предназначенном для его воспроизведения приложении - достаточно воспользоваться утилитой Fresh View. Данная программа позволяет осуществлять предпросмотр самых разных мультимедийных данных, включающих графические изображения, музыкальные файлы или видеоролики. Причем, все это можно делать в режиме слайд-шоу, если таковых файлов набирается достаточно много. Помимо предпросмотра имеются и такие функции, как печать файлов (относится к картинкам) и создание альбома в виде HTML страницы. Для работы с программой требуется бесплатная регистрация, после которой регистрационный код высылается по электронной почте.

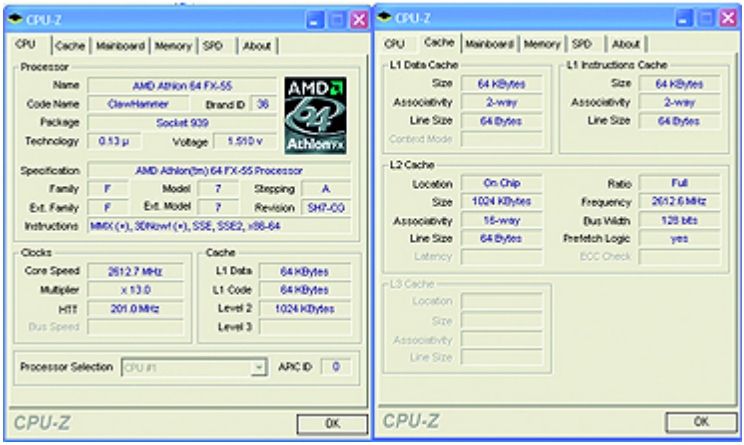
Шапка-невидимка



ОС Windows
www.v7soft.net
Версия 3.5
Размер 753 Кбайт
Интерфейс многоязычный (русский не поддерживается)
Цена $25.95
Ознакомительный период 3 дня

Для безопасной работы в Сети, при которой пользователь может быть почти уверенным в том, что очередной сеанс не создаст проблем, существует масса средств "предохранения", начиная от антивирусных программ и заканчивая файрволлами. Однако, чтобы обезопасить вашу privacy от излишне любопытных сервисов или веб-сайтов, их недостаточно: нужно скрывать IP-адрес. С данной задачей легко справляется утилита с недвусмысленным названием Hide IP. Автоматически подключаясь через различные прокси-серверы, программа позволяет скрыть от посторонних глаз реальный IP-адрес вашего компьютера. К тому же, работа через прокси усложняет подключение к вам извне.

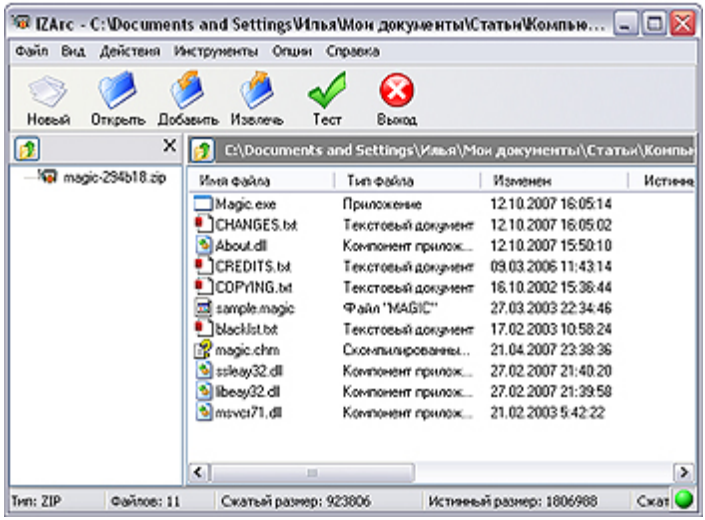
Препарируем процессор



ОС Windows
Адрес www.cpuid.com/cpuz.php
Версия 1.41
Размер 489 Кбайт
Интерфейс многоязычный (русский не поддерживается)
Цена бесплатно
Лицензия проприетарная (freeware)

Пожалуй, важнейшей частью компьютера является процессор, так что сведения о том, какое "сердце" бьется в вашем железном друге, могут оказаться весьма полезными. Узнать же максимум информации о процессоре можно с помощью небольшой, не требующей установки утилиты CPU-Z. Она сообщит вам марку чипа, имя изготовителя, напряжение питания ядра, характеристики кэша, наборы поддерживаемых инструкций и многое другое. С помощью CPU-Z можно определить, работает процессор на штатной тактовой частоте или подвергся разгону. Кроме того, программа выводит на экран информацию о материнской плате, состоянии памяти и системных компонентах.

Великий упаковщик


IZArc - C:\Documents and Settings\Илья\Мои документы\Статьи\Компью...
Файл Вид Действия Инструменты Опции Справка
Новый Открыть Добавить Извлечь Тест Выход
C:\Documents and Settings\Илья\Мои документы\Статьи\Компь
magic-294b18.zip
Имя файла Тип файла Изменен Истине
Magic.exe Приложение 12.10.2007 16:05:14
CHANGES.txt Текстовый документ 12.10.2007 16:05:02
About.dll Компонент прилож... 12.10.2007 15:50:10
CREDITS.txt Текстовый документ 09.03.2006 11:43:14
COPYING.txt Текстовый документ 16.10.2002 15:38:44
sample.magic Файл "MAGIC" 27.03.2003 22:34:46
blacklist.txt Текстовый документ 17.02.2003 10:58:24
magic.chm Скомпилированны... 21.04.2007 23:38:36
ssleay32.dll Компонент прилож... 27.02.2007 21:40:20
libeay32.dll Компонент прилож... 27.02.2007 21:39:58
msvcr71.dll Компонент прилож... 21.02.2003 5:42:22
Тип: ZIP Файлов: 11 Сжатый размер: 923806 Истинный размер: 1806988 Сжат

ОС Windows
Адрес www.izarc.org
Версия 3.81
Размер 3,6 Мбайт
Интерфейс многоязычный (русский поддерживается)
Цена бесплатно
Лицензия проприетарная (freeware)

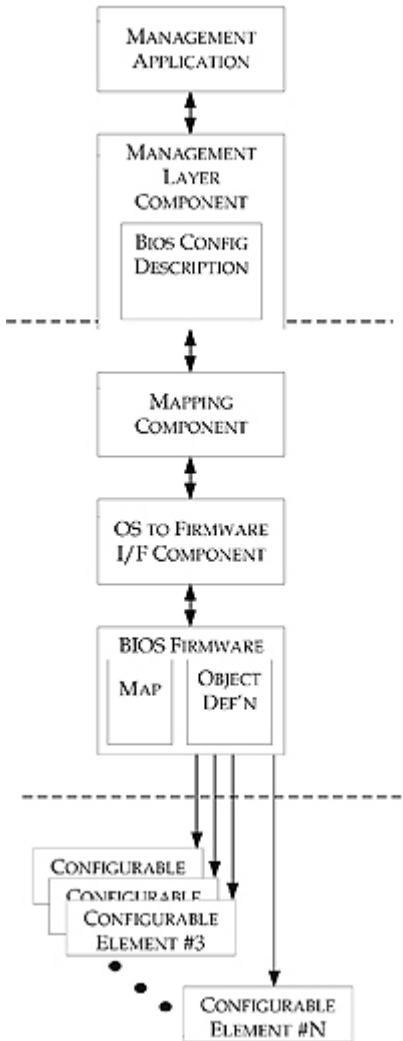
Архиватором сегодня никого не удивишь: любое известное приложение из этой категории обладает массой функций, практически полностью отвечающей запросам большинства владельцев ПК. Но не стоит упускать из виду и альтернативные программы-архиваторы, ведь не исключено, что в одной из них окажется именно тот набор функций, который удовлетворит ваши запросы на все 120%. Возьмем, к примеру, утилиту IZArc, разрабатываемую Иваном Захарьевым. Помимо внушительного списка поддерживаемых форматов, она может похвастаться такими полезными функциями, как создание защищенных паролем и разбитых на несколько частей архивов, подключение произвольных антивирусных сканеров, работа с самораспаковывающимися архивами и пр.

Патентное бюро

Автор: Сергей Леонов

Метод конфигурирования BIOS

Microsoft

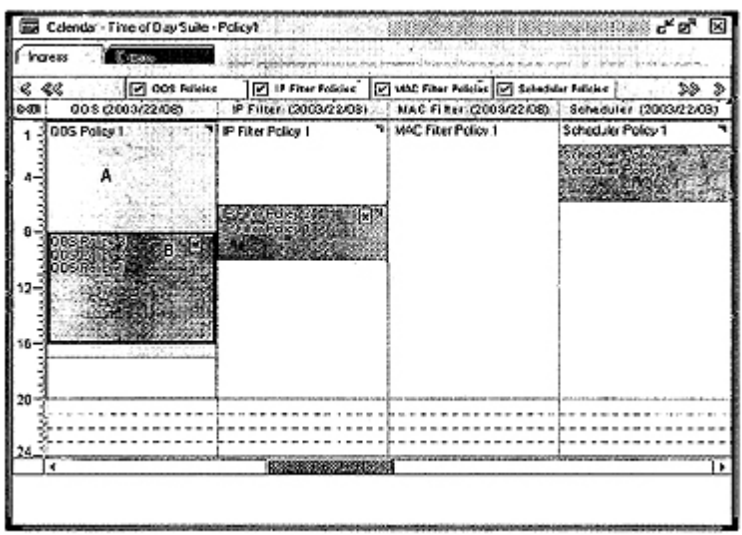


Небезызвестная компания решила внедриться на ранее недоступный ей низший уровень программного обеспечения, а

именно - в сферу конфигурирования параметров BIOS, сделав свою версию программы BIOS Setup. Проблема лишь в одном - так как BIOS собирается из модулей производителями, да и сами модули выпускаются как минимум тремя основными разработчиками, общего формата или хотя бы описания настраиваемых параметров не существует. В связи с этим предлагается создать некое описание элементов BIOS, подлежащих конфигурированию, дабы по этому описанию программа могла распознать тип элементов и корректно ими управлять. Остается мелочь - заставить разработчиков железа внедрить эту технологию, но к таким приемчикам небезызвестной компании не привыкать.

Календарь для сисадмина

Alcatel

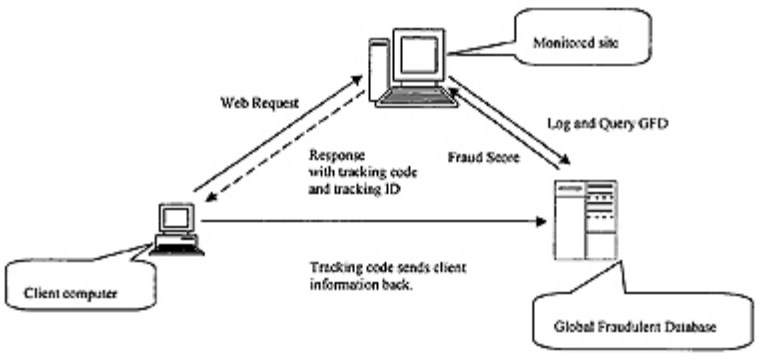


Системные администраторы - народ забывчивый, особенно по части создания резервных копий носителей или оплаты продления лицензий на программные продукты. Специально для них Alcatel предлагает сделать программный календарь наподобие примененного в MS Outlook, куда и будут (будут ли?) предварительно записываться все необходимые действия. "Заявки" в календарь могут вносить или сами администраторы (ох, свежо предание…), или программное обеспечение, которое требует обслуживания, или же пользователи, желающие получить толику внимания админа. Различные цвета могут отображать задачи для

разных рабочих станций в сети или важность запланированных действий. Графический интерфейс предусматривает даже отображение длительности работ по конкретному мероприятию, дабы админ мог правильно спланировать свой рабочий день.

Система определения некорректных кликов в реальном времени

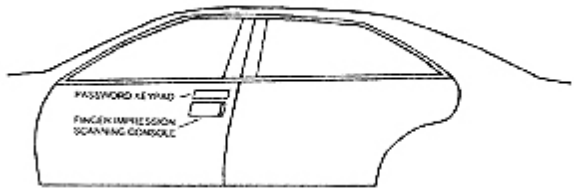
США



Компании, размещающие свою рекламу в Интернете, весьма обеспокоены активно развивающимися технологиями "накрутки" кликов - этим способом их реально "разводят на бабки", имитируя активность просмотра пользователем рекламы, когда таковой на самом деле нет. Для определения подобных действий в реальном времени предлагается создать систему-арбитр, определяющую "качество клика". Для определения "неправильного" клика арбитр должен сравнить лог-файл действий пользователя (нажатие кнопки мыши или клавиши Enter, перемещение указателя мыши над рекламным баннером или прочие действия, показывающие реальную активность) с лог-файлом сервера и при несовпадении - не засчитывать клик. Весьма сомневаюсь в перспективе этого предложения: мало того что отдавать на сторону протокол своих действий вряд ли кто захочет, так еще и сформировать подобный лог-файл программе, "накручивающей" клики, - пара пустяков.

Умный автомобиль

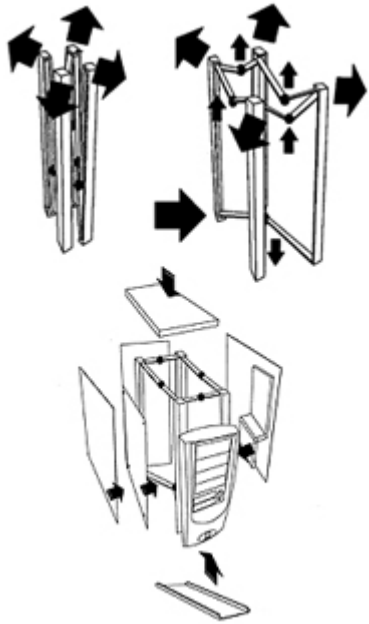
США



Очередная заявка на патент от женщины. Похоже, ей частенько приходится "арендовать" машину у мужа (или еще кого-нибудь), ибо суть заявки заключается в некоем устройстве, обеспечивающем автоматическую адаптацию всех возможных параметров авто под себя. Причем для активизации системы не нужно даже садиться в машину - в ручку водительской двери предлагается встроить сканер отпечатка пальца, и за время, пока водитель заносит ногу, прежде чем сесть в машину, автоматика должна отрегулировать высоту и наклон сиденья, положение руля и углы зеркал заднего обзора, установить нежное значение температуры на регуляторе климат-контроля, включить радио или другой источник звука и выбрать нужную станцию или соответствующий плейлист, загрузить в навигатор соответствующие пользователю точки назначения и маршруты, а во встроенный автомобильный телефон - персональную книгу контактов. Уф… кажется, все… Нет, не все. Автомобильный компьютер должен также настроиться на получение электронной почты с соответствующего адреса. В принципе реализовать вышеперечисленные функции не составит труда, но никаких подробностей, относительно того, как это сделать, в заявке нет - не женское дело копаться в мелочах.

Складывающийся компьютерный корпус

Тайвань



Как известно, транспортировка корпуса компьютера - процедура не самая удобная. Копеечный, по сути, корпус занимает много места, а значит, заметно возрастают расходы на транспортировку, хотя перевозится по большей части не железо, а воздух. Что касается стенок и передней панели корпуса, то здесь все нормально, они снимаются и много места не требуют. А вот каркас… Авторы заявки предлагают сделать каркас складывающимся, снабдив ребра шарнирами. В сложенном состоянии конструкция занимает гораздо меньший объем, а жесткость в разложенном виде обеспечивается за счет крепежных элементов стенок и передней панели.

TERRALAB.RU: Железный поток

Автор: Сергей Леонов

Fujitsu Siemens ESPRIMO Mobile U9200/M9400/D9500: Портативные компьютеры

Линейка бюджетных моделей ESPRIMO Mobile V призвана обеспечить оптимальное соотношение цена/производительность. Главной отличительной чертой модели U9200 называется тонкая и легкая (1,8 кг) конструкция. Ноутбук оснащен 12,1-дюймовым дисплеем. Модель M9400 имеет 14,1-дюймовый экран и весит 2,2 кг. D9500 с 15,4-дюймовым дисплеем и полноразмерной клавиатурой (вес 2,5 кг) вполне способен заменить настольный ПК. Все модели снабжены интегрированным модулем UMTS/ HSDPA и беспроводным сетевым адаптером. Наличие второй батареи позволяет работать до 8 часов без внешнего источника питания. Во всех ноутбуках используются одинаковые аксессуары, такие как репликатор портов и вторая батарея.

Fujitsu Siemens Lifebook S7210: Портативные компьютеры

Модель, которую производитель характеризует как профессиональный мобильный ПК, оснащена модулями мобильной связи стандартов UMTS и HSUPA для скоростной передачи данных. Она построена на базе процессора Intel Centrino Duo и набора микросхем Intel 965GM, диагональ экрана - 14,1 дюйма, вес 2,2 кг. Благодаря дополнительной батарее и кнопке EcoButton, при нажатии которой снижаются тактовая частота процессора и яркость экрана, ПК способен работать "в течение всего рабочего дня". Упоминается также клавиатура с защитой от пролитых жидкостей.

Defender Diamond 19: Акустическая система

Динамики 4” НЧ + 1” ВЧ (18 Вт RMS)
Диапазон частот 50-20000 Гц
Регулировки громкость, тембр ВЧ, тембр НЧ
Габариты 155x165x225 мм

Обладая техническими характеристиками колонок среднего уровня, Defender Diamond 19 выделяется главным образом своим необычным дизайном - деревянный серебристо-черный корпус подчеркивает белоснежные динамики в черно-"никелированном" обрамлении. Дополнительной особенностью колонок являются разъем для наушников, удобное управление и магнитная экранировка корпуса.

Point of View GeForce 8800 GT: Видеоускоритель

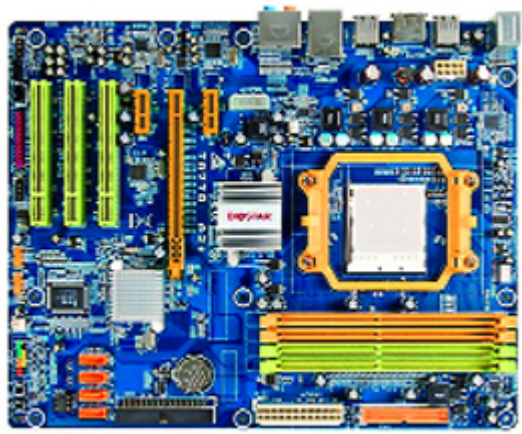
Новая модель графического адаптера так и называется - GeForce 8800 GT. Позиционируется устройство как сбалансированное решение для игр и обработки HD-видео. Новинка оснащена 512 Мбайт памяти DDR3, работающей на частоте 1800 МГц, и 256-разрядной шиной памяти, частота ядра 600 МГц. Разумеется, ускоритель поддерживает все функции графического ядра, на котором базируется: SLI, шейдеры модели 4.0, DirectX 10 и пр. О цене сказано лишь, что она весьма привлекательна.

Transcend JetFlash T3: Ультратонкий USB-накопитель

Габариты этой флэшки всего лишь 30,2x12,3x2,4 мм при весе 2 грамма. Для достижения такой толщины компания применила не традиционные микросхемы памяти, а бескорпусные чипы, монтируемые непосредственно на плате. Как сообщается, сломать поликарбонатовый корпус этого устройства при нормальной эксплуатации невозможно. Устройство выпускается в версиях на 1

и 2 Гбайт и поддерживает весь набор программных утилит Transcend, включающий в частности сжатие и шифрование (AES) данных Secret-Zip, возможность применения в качестве электронного ключа для компьютера, синхронизацию и прочее. Гарантия пожизненная, цена не приводится.

Biostar TA770 A2+: Системная плата



Поддержка процессоров AMD Phenom/Athlon 64 X2/64/FX/ Sempron

Чипсет AMD 770 + SB600

Интерфейсы USB 2.0 10

Интегрированный звук 8+2 канала HD Audio

Новинка T-серии, базирующаяся на чипсете AMD 770, поддерживает будущие процессоры AMD Phenom, двухканальную память DDR2-1066 и имеет возможность оверклокинга. Примененный чипсет реализует поддержку технологии HyperTransport 3.0 и шины PCI Express 2.0.

Gigabyte GV-NX88T512H-B: Видеоускоритель

Новинка базируется на графическом процессоре GeForce 8800 GT, имеет 512 Мбайт памяти GDDR3 и поддерживает шину PCI-Express 2.0. О частотах процессора и памяти не сообщается. Адаптер снабжен двумя интерфейсами Dual-Link DVI, поддерживающими два монитора с разрешением 2560x1600. В комплект поставки включена ролевая игра Neverwinter Nights 2. О цене новинки не сообщается.

Creative SoundWorks Radio CD 745/705: Радиоприемники/ стереосистемы

Компания расширяет спектр продукции, выпуская на рынок теперь уже и радиоприемники под своим брэндом. SoundWorks Radio CD 745 - универсальная компактная стереосистема со встроенным сабвуфером. AM/FM-тюнеры позволяют сохранить в памяти до 24 станций, а CD-проигрыватель с загрузкой через слот может воспроизводить форматы MP3/WMA и отображать названия треков. Имеется также два будильника и поддержка

RDS. Можно докупить док-модуль для iPod и управлять всей системой с помощью пульта дистанционного управления. SoundWorks Radio 705, выполненный в стиле ретро, имеет "специально разработанный динамик с воспроизведением всего диапазона частот".

ActePower AP UC-4Ж: Система автономного питания

Тип аккумулятора литиевый 50 Вт·час
Входное напряжение/ток 12,8 В/1,5 А
Выходные напряжения/ток 16,5/19/22 В/2,5 А макс.,
5 В/1,5 А макс.
Габариты 154x102,5x22,5 мм

От этого универсального аккумулятора можно питать ноутбук или другую портативную технику, независимо от того, функционирует или нет собственный встроенный аккумулятор питаемого устройства. Новинка совместима с любым ноутбуком, напряжение питания которого находится в диапазоне 16–24 В. Кроме того, она обеспечивает напряжение 5 В для USB-совместимых устройств. Цена не приводится.

iBASE MB930: Системная плата

Возьмите под козырек: это не бытовая, а промышленная ATX-плата на чипсете Intel Q35/ICH9 с поддержкой шины ISA (!). Как сообщается, это первая в мире подобная комбинация. Плата поддерживает процессоры Core 2 Quad, Core 2 Duo или Celeron с шиной 1333/1066/800 МГц и оперативную память DDR 2 800 МГц. Слот ISA добавлен для поддержки периферийных плат старого типа, которые до сих пор используются в промышленной автоматике в целях цифрового и аналогового ввода/вывода. Помимо этого, на плате есть четыре слота традиционного PCI, слот PCI-Express x1 и PCI-Express x16. Поддерживается до шести коннекторов SATA (с возможностью объединения дисков в RAID-массив), три порта RS-232, один RS232/422/485 и восемь каналов USB 2.0. Сетевые интерфейсы представлены двумя каналами Gigabit Ethernet. Имеются встроенные "сторожевые" таймеры (WatchDog), избавляющие пользователей от необходимости выделения отдельных слотов под таковые.

Toshiba Satellite A200-1M8/1KH: Портативные компьютеры

Ноутбуки с предустановленной Windows Vista позиционируются как универсальные машины для решения повседневных задач в офисе и дома. Модели выполнены в блестящем темно-синем корпусе. A200-1M8 скрывает внутри процессор Core 2 Duo T7100 с тактовой частотой 1,8 ГГц и кэш-памятью второго уровня 2 Мбайт, 1024 Мбайт памяти, жесткий диск на 160 Гбайт и привод DVD Super Multi с поддержкой двухслойной записи. A200-1KH - более мощная конфигурация с процессором Core 2 Duo T7300 (2.0 ГГц), 2048 Мбайт оперативной памяти, диск емкостью 300 Гбайт, а также привод HD DVD. Компания сообщает, что прогнозирует повышение спроса на эти модели и готовит большую партию. Относительно цены сказано лишь, что она "вполне доступная".

огород козловского: А я говорю: налево!

Автор: Козловский Евгений

Гуляя по форумам, посвященным GPS-навигации, я все чаще встречаю упоминание программы Navitel (www.navitel.ru - правда, с этого адреса вас направляют на www.navitel.su, но обещают, что скоро перестанут). Пристрастие к ней питают в основном провинциалы: из серьезных навигационных программ практически у одной лишь Навител есть и подробная, с ведением по маршруту, карта Нижнего Новгорода, и карты Екатеринбурга и Свердловской области, Новосибирска и Новосибирской области, карты Самары, Челябинска, Кургана, Курганской области, а также Уфы, Белогорода, Кемерово, Тюмени, - не говоря о Москве и Питере с их областями… Это, конечно, далеко не вся Россия, но куда ближе к ней, чем карты iGO или Tomtom'а, и, надо полагать, у Навителa есть все возможности и шансы впереди них оставаться и впредь, тем более что, в отличие от некоторых соотечественных коллег-конкурентов, они пользуются не одинаковыми у разных программ картами Телеатласа, а своими, посконными и домоткаными.

Вообще говоря, есть у Навителa и бесплатная карта всей территории России. Насколько "всей" - проверить не удалось (это надо недельку просидеть с программой и тыкать, тыкать, тыкать…), но так или иначе, близкие мне города вроде Омска, Приморска или Шадринска я обнаружил: не в полной, конечно, детализации, но основные улицы все-таки просматриваются. Оно и понятно: карта общая, обеспечивающая, скажем так, транзит. И с нее довольно. А что надо подробнее - есть отдельно или (надеюсь) скоро будет. Кроме того, для Навителa существует конвертор и редактор карт, так что многое, - если есть в каком-то формате, - можно адаптировать, а то и "нарисовать" с нуля.

После знакомства с PalmGIS и "Автоспутником" я стал слегка опасаться отечественных навигационных программ - и все же решил рискнуть еще раз. Скажу сразу: мне программа понравилась. У нее есть много дефектов, но они, по моему разумению, устраняются без особого труда. Считая на сегодня образцом навигационных программ iGO, я обнаружил очень мало (не слишком существенных) позиций, по которым Навител ей уступает (например, по красоте графики или отсутствию

специальных, отдельных, кнопок "Дом" и "Работа"), - зато обнаружил несколько (для меня) новинок, которых и iGO, и Tomtom лишены. Например, если вы вручную увеличите или уменьшите карту, две названные программы практически тут же вернут вас в автоматически выставляемый масштаб, что не всегда совпадет с вашими планами, - у Навителa же при изменении масштаба вручную тут же появляется иконка, нажав на которую (и только в этом случае!) вы возвращаете автоматический режим. Есть и отдельная иконка для возврата на актуальное местоположение, - что удобно, если вы, остановившись на минутку, решили посмотреть какие-то сравнительно (или даже несравненно) дальние места карты. Решена давным-давно раздражавшая меня (в "Автоспутнике", например) проблема излишней детализации: когда масштаб уменьшается, ни контуров, ни номеров домов не видать, - при подъезде же к месту назначения (где они нужны) - они появляются [К тому же уровень детализации можно задать в настройках]. Прокладка маршрута тоже куда проще и очевиднее, чем у именитых иноземцев, - да можно найти еще кое-какие приятности: например, более чем достаточное количество информативных настраиваемых датчиков: больше чем даже у iGO. И это при том, что почти все базовые (для меня) способности программы реализованы не хуже, чем у иностранцев: и автоматическая смена дня/ночи, и автоматическое масштабирование, и выбор ориентации карты - на север, по маршруту, по движению… Ну, то есть чуть-чуть подлизать графику, поправить десяток багов (есть баги, есть!) - и программа окажется вполне конкурентоспособной, без скидок.

Главное же достоинство, которое может заставить многих сегодняшних московских и питерских пользователей Tomtom'а и iGO (вроде, например, меня) перейти на Навител, - это адресная база, включающая не только номера домов, но и их корпуса, строения и тому подобные отечественные изощренности. Возможно, конечно, что и Tomtom с iGO когда-нибудь до этого дойдут, но вряд ли: они сегодня и простых номеров домов в Москве не знают изрядное количество [Навител, впрочем, не знает, например, моего автосервиса по адресу Севастопольский проспект, 95 Б. Причем не только "Б" - но и 95 вообще, и ни одного дома из девятого десятка]. К тому же Навител "понимает" пробки от "Смилинка", и хотя качество этой "пробочной" информации продолжает оставаться малоудовлетворительным, семидолларовая месячная цена подписки более или менее адекватна сервису. (Этими же достоинствами привык кичиться и "Автоспутник", - однако они сопровождаются таким числом недостатков, что я предпочитал без них обходиться; в случае же с

Навителом появляются реальные шансы на предпочтение. Правда, от iGO отказаться совсем не получится: в отличие от этой программы, Навител не расставляет [пока?] информацию о камерах, измеряющих скорость, что может при каких-нибудь загородных поездках обойтись весьма дорого.)

Вообще программа после загрузки сильно напомнила мне GIS RUSSA, к которой я всегда относился тепло, сознавая, что у этой самоделки и не может быть полного набора привычных мне возможностей, - зато огромный (сравнительно с иноземцами) ассортимент российских карт и неплохие программные идеи: та же иконка спутника (с тем же голоском: "Соединение со спутниками установлено"), то же ведение по вектору, если нет или неизвестны дорожки [Тут же уж замечу, что у Навителa, как и у GIS RUSSA (как, впрочем, и у "Автоспутника"), хотя московские дома прорисованы чуть ли не все, подъездные дорожки к ним и проезды между ними почему-то не обозначены, - и вот тут-то и вступает в силу Вектор, - впрочем, Tomtom и iGO в подобных случаях попросту пасуют: неизвестно, дескать, где вы находитесь!]. И впрямь: как мне объяснили, генезис у этих программ один и тот же, так что интуиция не подвела.

Но будем считать, что комплиментарная часть "Огорода" завершена, и перечислим замеченные в первый же день пользования баги: не столько поворчать, сколько в надежде, что программисты прочтут и хоть кое-что, да исправят.

Про отсутствие иконок "Дом" и "Работа" я уже написал. Про отсутствие дорожек между домами - тоже. Исправление последнего, конечно, требует добавочной и немалой работы, - однако, коль уж знаем все дома и строения, - надо покрыть и это белое пятно.

Далее: работа со "Смилинком". Чтоб получать от него информацию о пробках с заданной периодичностью, надо с нею же выходить в Интернет. Нормальные, правильные программы, не обнаружив Интернета по WiFi-каналу или по ActiveSync'у, сами запускают GPRS. Эта, увы, нет, и приходится вручную вызывать какую-нибудь "нормальную", вроде Pocket IE или "Оперы", чтобы инициировать GPRS-соединение, - и лишь тогда "пробки" обновятся [Для Windows Mobile 6. Для "пятерки" такие проблемы когда возникают, а когда и нет. Что называется - через раз.]. Но даже когда ты в Интернете, "пробки" все равно время от времени заклинивают. Позвонив в диспетчерскую службу "Смилинка", я выяснил, что эта проблема с Навителом у них давняя: при проверке, что ли, легальности программа сбрасывает какой-то код - и восстанавливать его оператору "Смилинка" приходится вручную. Что и было сделано в полминуты, - однако на вопрос:

нет ли способа попроще, чем всякий раз звонить по телефону, мне ответили, что нет и что, дескать, обращайтесь в Навител. Обращаюсь!

Далее: проблема, перешедшая к Навителу от GIS RUSSA. Не говоря уж о несанкционированном выходе из навигатора (такое порой поневоле, при нечастых, но все же бывающих зависаниях или случайно случается) - "спутниковый" модуль не выгружается и при повторной загрузке программы (или какого-нибудь другого навигатора) его сигналы не воспринимаются. В результате приходится делать полную перезагрузку КПК.

Далее: при поиске дома с корпусами и строениями по адресу, вам выводится список этих самых корпусов и строений - и порой (не всегда) пункты списка налазят один на другой. Разобрать, в общем, можно - но как-то… неаккуратненько. Неаккуратненько и то, что мне не удавалось удалить случайные "путевые точки" из меню, - только непосредственно с самой карты. Но, повторю, - это мелочи, которые легко правятся и будут поправлены без сомнения.

А вот последний недостаток… Увы, при первом же выезде, на расстоянии около десяти километров, Навител настоятельно призвал меня грубо (с лишением прав!) нарушить правила движения раза четыре. Сначала он приказал повернуть с Комсомольского налево, на 3-ю Фрунзенскую, - что на этом перекрестке запрещено, сколько я себя помню за рулем: для левого поворота надо заехать в карман и из него уже пересечь Комсомольский. Затем, при движении по Большой Пироговке, он дважды звал меня повернуть налево - ровно напротив знаков "только прямо". И напоследок приказал непосредственно повернуть с проспекта Вернадского на Удальцова, где я живу. Такой поворот запретили уже больше двух лет назад. Когда я поехал все-таки прямо, Навител предложил свернуть в узенький проезд, чтобы, объехав кинотеатр "Звездный", выбраться на Удальцова и проспект Вернадского пересечь. Неплохая идея, ее, помнится, и "Автоспутник" предлагал, - но не учитывающая реалий: из двора за "Звездным" выехать на Удальцова - это та еще песня, которая может звучать до получаса (преувеличиваю, но чуть-чуть), и столько же потом простоять у светофора. Я снова поехал прямо и обнаружил, что Навител превосходно знает "правильный" разворот на проспекте (через который, и только через который всю жизнь ведут меня домой и Tomtom, и iGO), - но предлагает его только в третью очередь. Зато Навител категорически не знает, например, двухлетнего уже возраста Рамстора у метро "Университет": со сложной и разветвленной системой стоянок и выездов. Когда его не знают Tomtom и iGO -

это еще простительно: все-таки иноземцы. Ну а уж наши-то, которым и покататься по Москве - не задача, и изменения в карту внести - пустяк…

Правда, по поводу поворотов налево в запрещенных местах директор по маркетингу Навителa сказал, что это ошибка не столько программы, сколько его личная: он, дескать, выдал мне московскую карту последней версии, находящейся еще на стадии бета-тестирования. Я, конечно, плохо представляю себе, чтобы в новую версию не перенесли знаки из старой (хотя на примере FineReader'а уже знаю, что следующая версия вполне может оказаться сильно хуже предыдущей), - однако согласился поставить старую и проверить.

Проверка показала, что из четырех призывов к грубому нарушению ПДД остался только один, - и тот связан со знаком, установленным, кажется, недавно. Так что претензии почти снимаются, а мои изумления по поводу призывов "ехать налево" (один из которых я даже выполнил: благо ментов поблизости не оказалось!) будем считать копеечкой в копилку бета-тестирования нового варианта карты Москвы.

письмоносец: Холодным субботним ноябрьским утром

Автор: Илья Щуров Voyager

Холодным субботним ноябрьским утром я из дому вышел, по важным делам. В это утро список подвигов включал в себя оплату "Стрима", покупку памперсов и поездку в Подмосковье за реанимированным ноутбуком.

Утро выдалось с бодуна. Накануне вечером я пил водку и пиво. Тем вечером я выпивал с друзьями. Я встречался с друзьями, с которыми пятнадцать лет назад учился в МЭИ. Ореол советского академического образования, который перешел с вечера на утро, делал факт наличия бодуна как бы незначительным.

Тем не менее в голове вертелась мысль - а не купить ли пива на лишние сверхбюджетные 50 рублей. Но при взгляде на киоск с прессой возникла конкурирующая идея - купить "Компьютерру".

Победила конкурирующая идея. По дороге к метро, на бодрящем ветру, я изучал синюю полоску с надписью IBM, в которую был завернут журнал, размышляя о специфике координации рук в условиях пониженной температуры, о советском академическом образовании, о корпорациях и об отделе рекламы, придумавшем заставить читателя отрывать этот рекламный носитель от журнала. Спустя двадцать минут я понял, что интуиция меня не подвела. Разглядывание фотографии Юджина Хутза на 37-й странице (#708) совершенно устранило какие-либо симптомы недомогания, а чтение журнала окончательно закрепило полученные положительные результаты.

Хотел бы выразить благодарность! Всей редакции.

Антон

От редакции: Могу порекомендовать более эффективный способ использования "Компьютерры" для лечения бодуна: употреблять ее не после, а вместо.

Вы пишете, что мы нанимаем дизайнеров, рекламщиков и прочую братию. Увы, окружающую нас среду эти люди формируют даже не пытаясь к нам наняться. Мы только оплачиваем их потуги в режиме бизнес-ланча: кушать хочется, поэтому мы здесь, но о выборе лучше забыть. Нет именно выбора (вам нужны примеры крайней монополизации и недружественной унификации целого ряда составляющих нашей окружающей среды?). Торговля кирпичём в подворотне отнюдь не является наймом поставщика кирпича. Так что сам термин "найм" не

стыкуется с предложением лишний раз подумать над своим кошельком. Я бы хотел нанять производителя телефона с полноценным BT, но без камеры и символьным ЖК-экраном (солнце, знаете ли). Или просто с флипом (мне такое очень нравилось). Ну и наконец любого водонепроницаемого "внедорожного" аппарата. Не подскажете, где искать подрядчиков? Я б нанял.<...> Вы начали там про "одну редмондскую компанию". Некая такая (же) не так давно нанялась в подрядчики к правительству Нигерии. От наших действий и вправду что-то (увы, совсем не всё) зависит, так вот в наших действиях сейчас, похоже, становится главным научиться не нанимать этих самых, которые так рьяно создают нашу среду. Если, конечно, есть желание задуматься, причем не только доставая кошелек.

Андрей Власенко

От редакции: Андрей, большое спасибо за письмо! Но мне все-таки кажется, что от нас зависит совсем все. Но это уже мировоззренческий вопрос, являющийся во многом предметом веры, нежели рационального обоснования. Как и подавляющее большинство вопросов, которые нас действительно интересуют.

Во врезке к статье преподобного Михаила Ваннаха "Экстрим для ученых" (#707) упоминается Николя-Жак Контэ (1755–1805), изобретатель современного карандаша, а также некоторых усовершенствований в области воздухоплавания. Однако не упоминается главное и, вероятно, секретное изобретение Конте - машина времени, благодаря которой "он в 1892 (!) году предложил использовать воздушные шары для наблюдения за противником, после чего и был назначен директором аэростатического института и начальником бригады аэронавтов".

В "Голубятне" в том же номере обсуждаются ноутбуки Sony Vaio, в которых "алюминиевый корпус заменен на углеводное (!) волокно, снижающее вес ноутбука при сохранении прочности". Не знаю, как насчет прочности, но питательность ноутбука при использовании углеводного, то есть скорее всего сахарного корпуса наверняка повысилась. А упомянутый в заголовке "Голубятни" загадочный лобзик, видимо, и нужен, чтобы отпиливать куски корпуса при отсутствии иных источников энергии (не для ноутбука, а для его хозяина).

Если серьезно, то подобные мелкие опечатки хоть и не мешают получать удовольствие от чтения журнала, но вызывают горячее желание немедленно оставить комментарий к статье, что в бумажном варианте "КТ", как и отметил Гуриев в "13-й комнате", пока невозможно. Засим остается "Письмоносец", что я и делаю.

Сергей "nem0"

От редакции: Мы давно подозревали, что Голубицкий и Козловский питаются гаджетами. В одном из недавних "Огородов" ("Так - люблю, а есть - нэт!") Евгений Антонович по этому поводу уже чуть не проговорился, но после вашего письма все становится совсем ясно. Раскусили, одним словом.

Призом награждается Андрей Власенко - за желание задуматься. Плеер Ritmix RF-7400 4G. Приз предоставлен компанией Ritmix.